Configuration et administration

Gestion utilisateurs

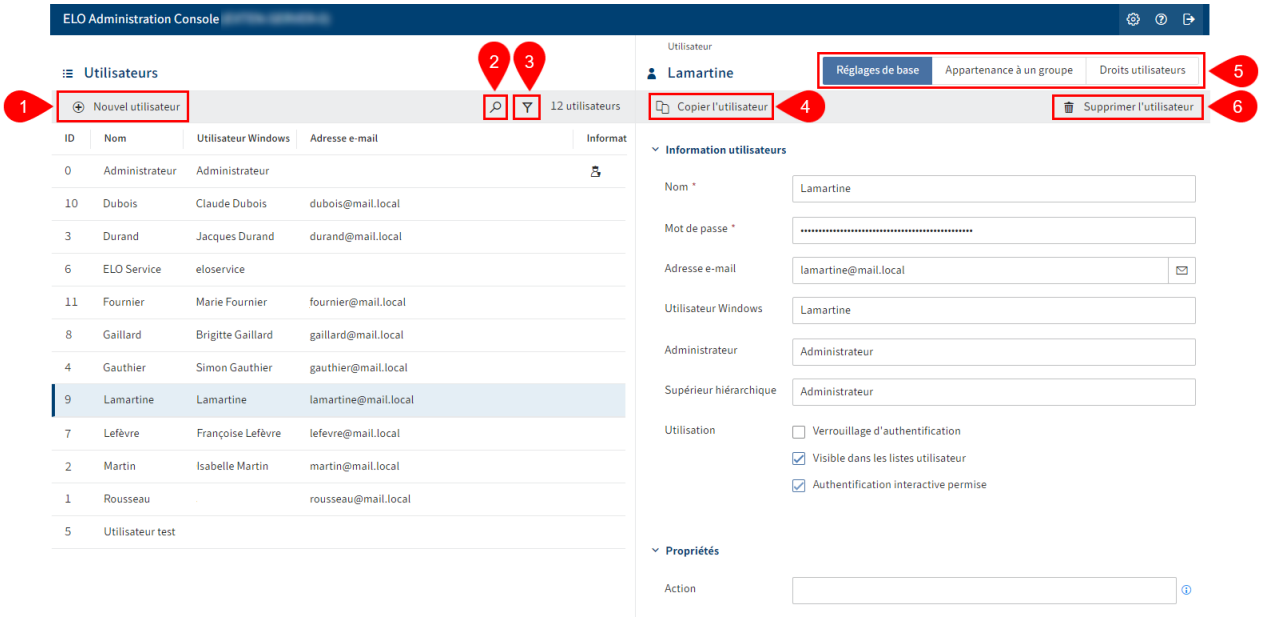
Table des matières

Utilisateur

Aperçu

Toutes les personnes qui utilisent ELO ont besoin d'un compte ELO correspondant. Ces comptes sont créés, configurés et administrés dans la gestion des utilisateurs.

Vous pouvez ouvrir la gestion utilisateur dans la console d'administration ELO via *Réglages système > Gestion utilisateurs*.



La gestion des utilisateurs propose les possibilités suivantes :

1 Créer un utilisateur

2 Effectuer la recherche

3 Définir un filtre

4 Copier un utilisateur : toutes les configurations sont copiées, sauf les champs *Nom*, *Adresse e-mail*, *Mot de passe* et *Utilisateur Windows*.

5 Effectuer la configuration : via les onglets Réglages de base, Appartenance à un groupe, Droits utilisateur

6 Supprimer un utilisateur

Supprimer l'utilisateur

> **Remarque**
>
> Lorsque vous supprimez un utilisateur, celui-ci sera supprimé définitivement.

Ne supprimez pas un utilisateur qui a déjà été utilisé dans ELO. Cela peut entraîner des inconsistances. Dans ce cas, il est mieux de ne pas supprimer l'utilisateur, mais de modifier le réglage de base :

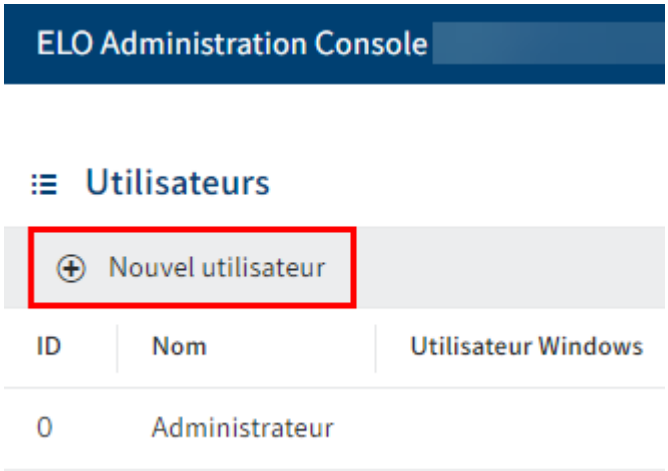
1. Activez *Activer le verrouillage d'authentification*
2. Désactivez *Permettre une authentification interactive*
3. Désactivez *Visible dans les listes utilisateur*

L'utilisateur ne peut plus s'authentifier à ELO et il ne sera plus visible pour les autres utilisateurs. Dans ELO, il n'est plus que disponible à l'arrière-plan. Ses actions passées, comme un fil d'actualité déjà rédigé ou une entrée dans les versions de document, sont encore visibles dans ELO.

Créer un utilisateur

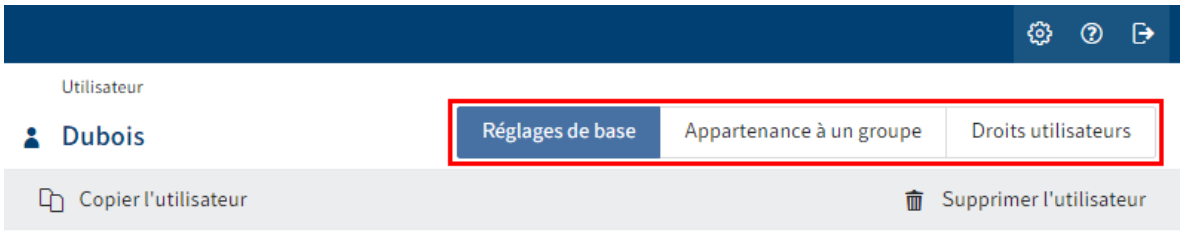
Pour créer un utilisateur, procédez de la manière suivante :

1. Veuillez ouvrir la console d'administration ELO.
2. Ouvrez la gestion utilisateurs (*Réglages système > Gestion utilisateurs*)



3. Sélectionnez *Nouvel utilisateur*.

   La section *Utilisateurs* apparaît.



4. Configurez le nouvel utilisateur. Naviguez vers le nouveau groupe via les onglets *Réglages de base*, *Assignation à un groupe* et *Droits utilisateur*.

   Vous trouverez d'autres informations à ce sujet dans le chapitre Configuration.

5. Une fois que vous avez effectué la configuration, sélectionnez *Enregistrer l'utilisateur*.

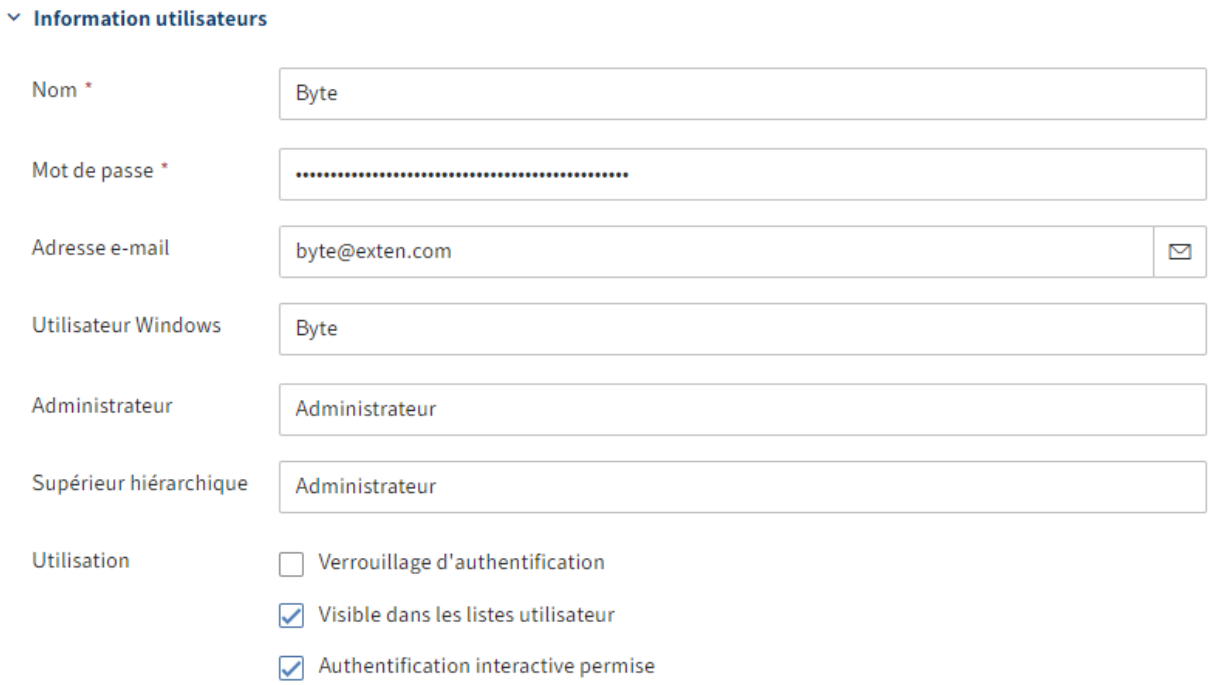
Vous avez créé un nouvel utilisateur.

Configuration

Déterminer les réglages de base

Dans la section *Réglages de base*, définissez les *Informations utilisateur*, les *Propriétés* et les *Informations supplémentaires*.

Information utilisateurs



- Nom : champ obligatoire. Peut être modifiée ultérieurement.
- Mot de passe : champ obligatoire. Peut être modifié ultérieurement.
- Adresse e-mail : est affichée dans le client dans le profil correspondant et elle pourra être utilisée dans des processus, des formulaires et scripts.
- Utilisateur Windows : si nécessaire, entrez le nom de compte Windows, par exemple, si vous souhaitez utiliser SSO. Cette information pourra être utilisée dans des processus, des formulaires et scripts.
- Administrateur : est rempli automatiquement avec le nom du compte avec lequel le nouvel utilisateur est créé. Si le compte possède le droit *Administrateur principal*, le champ *Administrateur* est rempli avec le compte *Administrateur*. Peut être modifié ultérieurement. Permet de déterminer qui a le droit de modifier les données de base de l'utilisateur correspondant.
- Supérieur : peut être utilisé dans des processus, formulaires et scripts. Le contenu du champ *Nom* est copié lorsque ce champ reste vide.
- Utilisation :
    - *Verrouillage d'authentification* : lorsque cette option est activée, une authentification au système ne sera plus possible avec ce compte. Le compte reste visible dans le système. Pour le masquer, désactivez le réglage de base *Visible dans les listes utilisateurs*.

> **Information**
>
> Cette option n'est pas disponible pour le compte *Administrateur*.

- *Visible dans les listes utilisateurs* : si cette option est activée, le compte apparait dans les listes de sélection dans le client ELO. Lorsque cette option est désactivée, le compte n'est visible que pour l'administrateur. Les actions déjà effectuées avec ce compte, comme les documents déposés ou les nouvelles versions de document, restent visibles pour tous dans le client ELO.

  > **Information**
  >
  > Les membres d'une unité d'organisation voient seulement les membres se trouvant dans leur unité d'organisation.

- *Authentification interactive permise* : lorsque cette option est activée, l'utilisateur peut s'authentifier au client ELO par le biais du dialogue d'authentification.

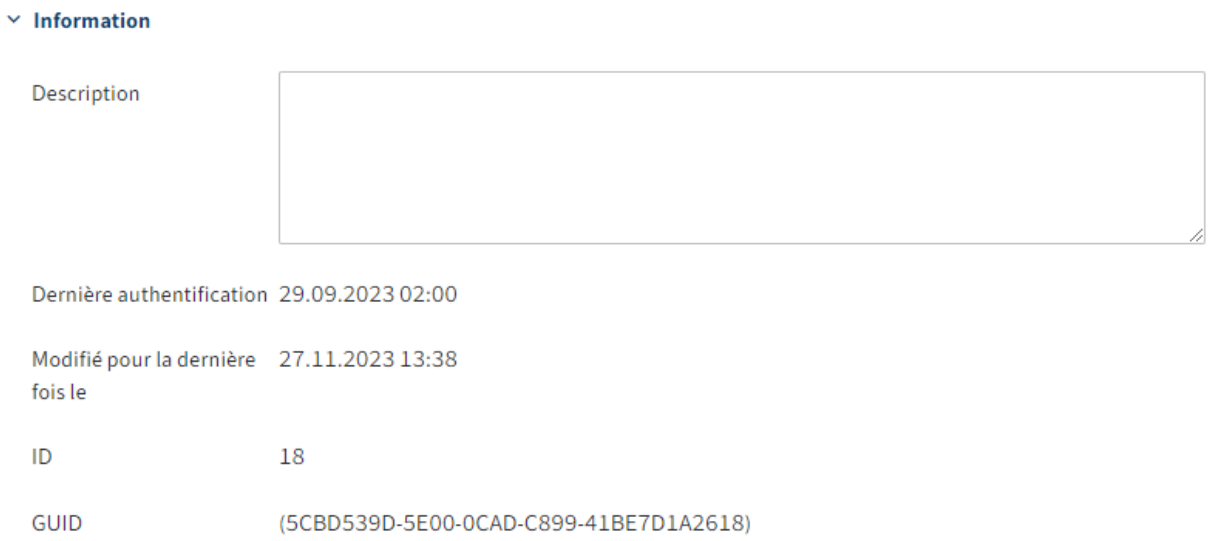
  > **Remarque**
  >
  > Ce réglage ne peut pas être vérifié par le serveur. Ce verrouillage ne peut pas être contourné.

  > **Information**
  >
  > Cette option n'est pas disponible pour le compte *Administrateur*.

Propriétés

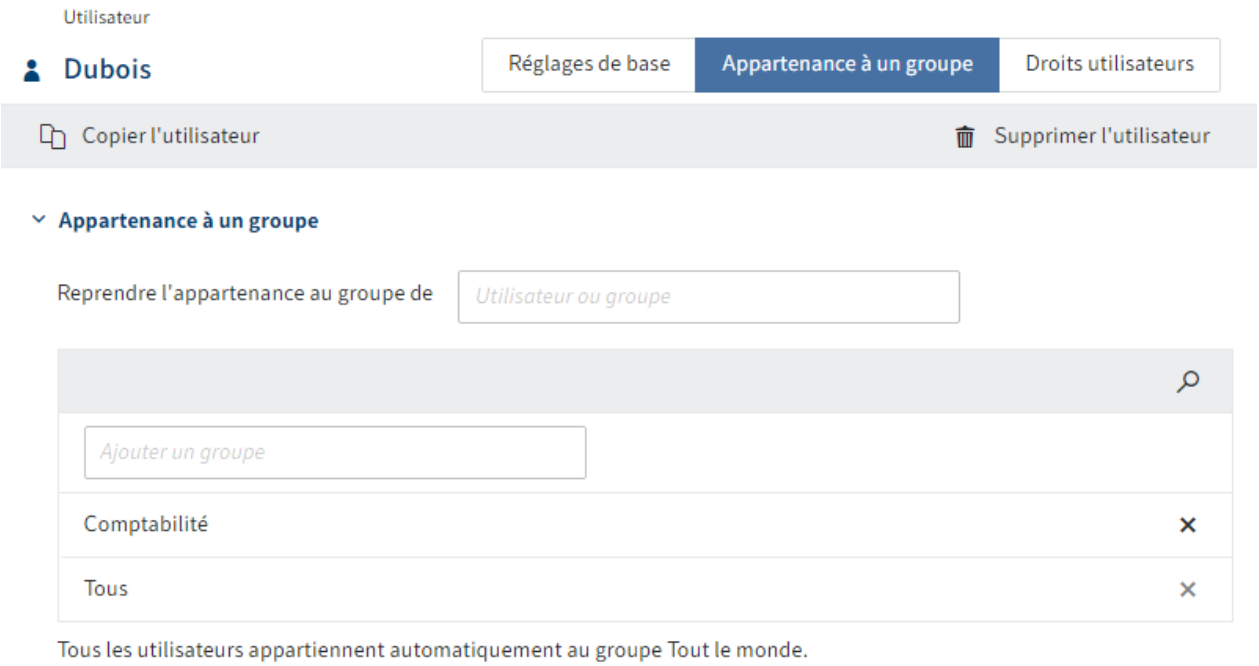
- Action : les raccourcis entrés ici ont un impact sur le mot de passe.
    - Exemples :
        - EX20223105 : le mot de passe expire le 31 mai 2023 et devra être renouvelé.
        - PW : le mot de passe défini peut être modifié lors de la première authentification.
        - PW : le mot de passe défini peut être modifié lors de la première authentification.
- Propriété 1-5 : les informations peuvent être analysées via des scripts.
- Unité d'organisation : vous trouverez des informations à ce sujet sous Configuration et administration > Gestion utilisateurs > Autres configurations > Unités d'organisation.

Information



- Description : le texte ne doit pas faire plus de 250 caractères.
- Dernière authentification notifiée : s'actualise automatiquement.
- Modifié récemment : s'actualise automatiquement
- ID : chaque compte obtient automatiquement un ID. L'ID peut être utilisé pour s'adresser au compte pour d'autres fonctions.
- GUID : chaque compte obtient automatiquement un GUID. Le GUID peut être utilisé pour s'adresser au compte pour d'autres fonctions.

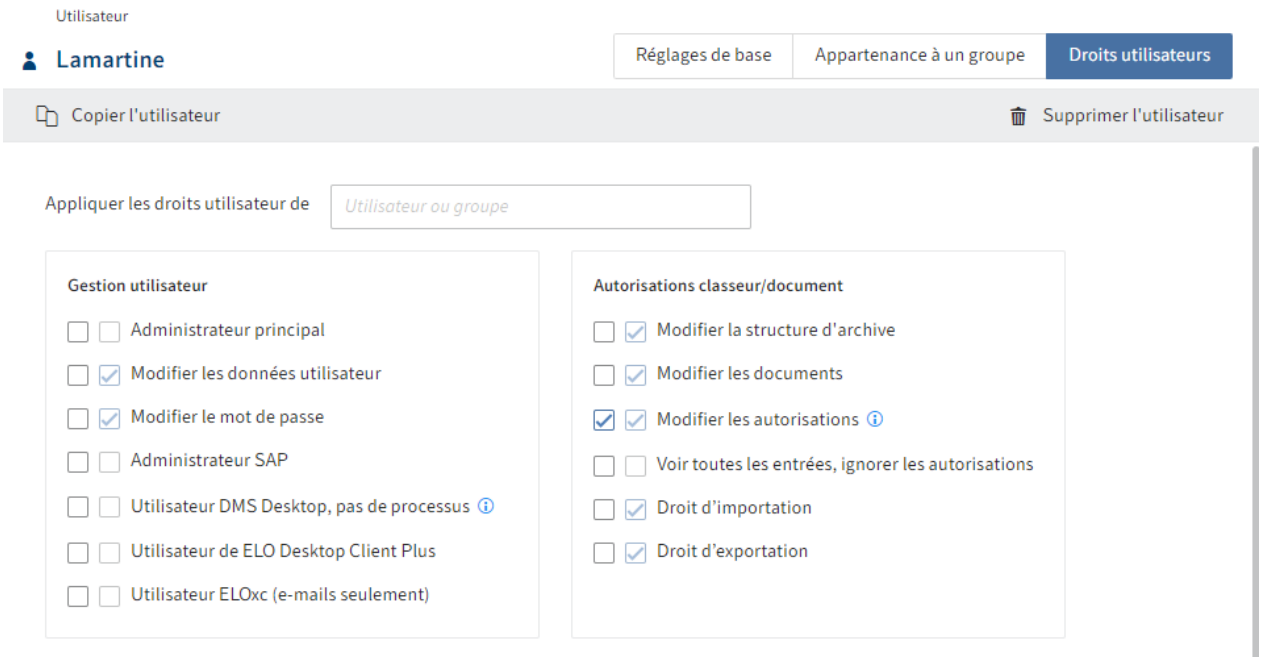
Définir l'appartenance à un groupe



Vous pouvez soit copier une appartenance de groupe existante d'un autre utilisateur ou d'un groupe manuellement. Vous pouvez ajouter un utilisateur à un ou plusieurs groupes. Les utilisateurs font toujours partie du groupe *Tout le monde*.

> **Information**
>
> Tapez un espace dans un des champs de saisie pour faire afficher l'intégralité de la liste des utilisateurs et groupes existants.

Assigner les droits utilisateurs



Il existe trois possibilités pour l'attribution des droits utilisateurs :

- Transmission

  Vous trouverez d'autres informations à ce sujet sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Leg de droits

- Assignation manuelle

  Vous trouverez d'autres informations à ce sujet sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Droits utilisateur

- Copier les droits utilisateur d'un autre utilisateur ou d'un groupe

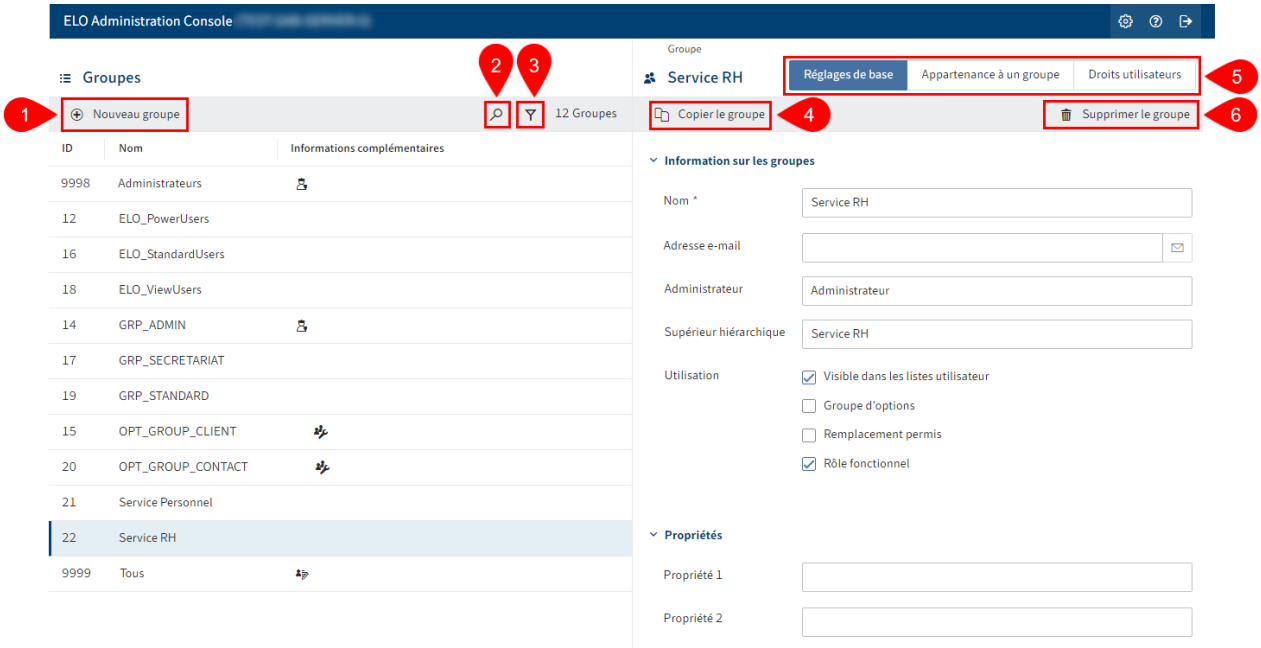
> **Information**
>
> Dans l'idéal, tous les droits seront légués via des groupes. Cela permet de simplifier considérablement l'assignation et l'administration des droits.

Groupes

Aperçu

Il est possible de gérer des droits, autorisations et réglages de base dans ELO via les groupes. Par ailleurs, les groupes sont utilisés dans les processus et pour les règles de remplacement.

La gestion des groupes s'ouvre dans la console d'administration ELO via *Réglages systèmes > Gestion des groupes*.



La gestion des groupes propose les possibilités suivantes :

1 Créer un groupe

2 Effectuer la recherche

3 Définir un filtre

4 Copier le groupe : toutes les configurations sont copiées, sauf les champs *Nom* et *Adresse e-mail* ainsi que les membres.

5 Effectuer la configuration : via les onglets 'Réglages de base', 'Appartenance à un groupe', 'Droits utilisateur'

6 Supprimer le groupe

Supprimer le groupe

> **Remarque**
>
> Si vous supprimez un groupe, celui-ci sera supprimé définitivement.

Ne supprimez pas de groupe qui a déjà été utilisé dans ELO. Cela peut entraîner des inconsistances. Dans ce cas, il est mieux de ne pas supprimer le groupe, mais de modifier le réglage de base.

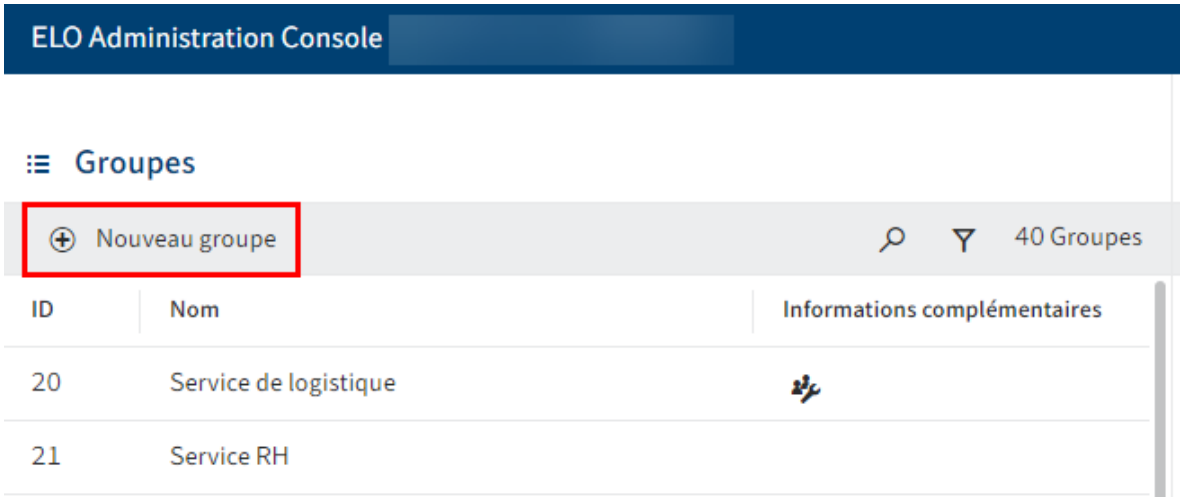
- Désactivez *Visible dans les listes utilisateur*

Ce groupe n'est disponible plus qu'à l'arrière-plan d'ELO. L'assignation des droits via le groupe reste et les actions précédentes avec ce groupe, comme des participations à des processus, sont encore visibles dans ELO.

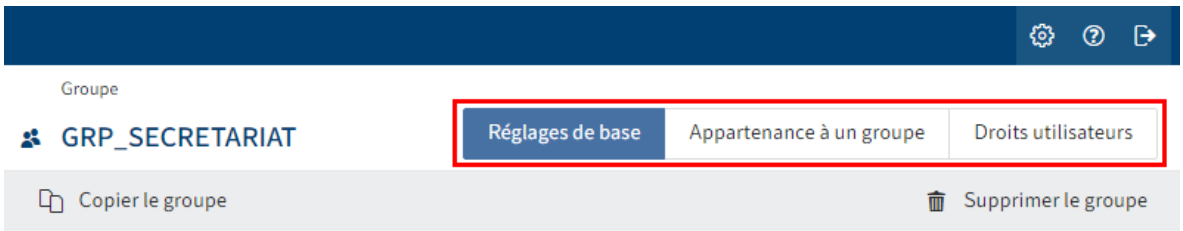
Créer un groupe

Pour créer un groupe, procédez de la manière suivante :

1. Veuillez ouvrir la console d'administration ELO.
2. Ouvrez la gestion de groupes (*Réglages systèmes > Gestion des groupes*).



3. Sélectionnez *Nouveau groupe*.



   La section *Groupe* apparaît.

4. Configurez le nouveau groupe. Naviguez vers le nouveau groupe via les onglets *Réglages de base*, *Assignation à un groupe* et *Droits utilisateur*.

   Vous trouverez d'autres informations à ce sujet dans le chapitre Configuration.

5. Une fois que vous avez effectué la configuration, sélectionnez *Enregistrer le groupe*.

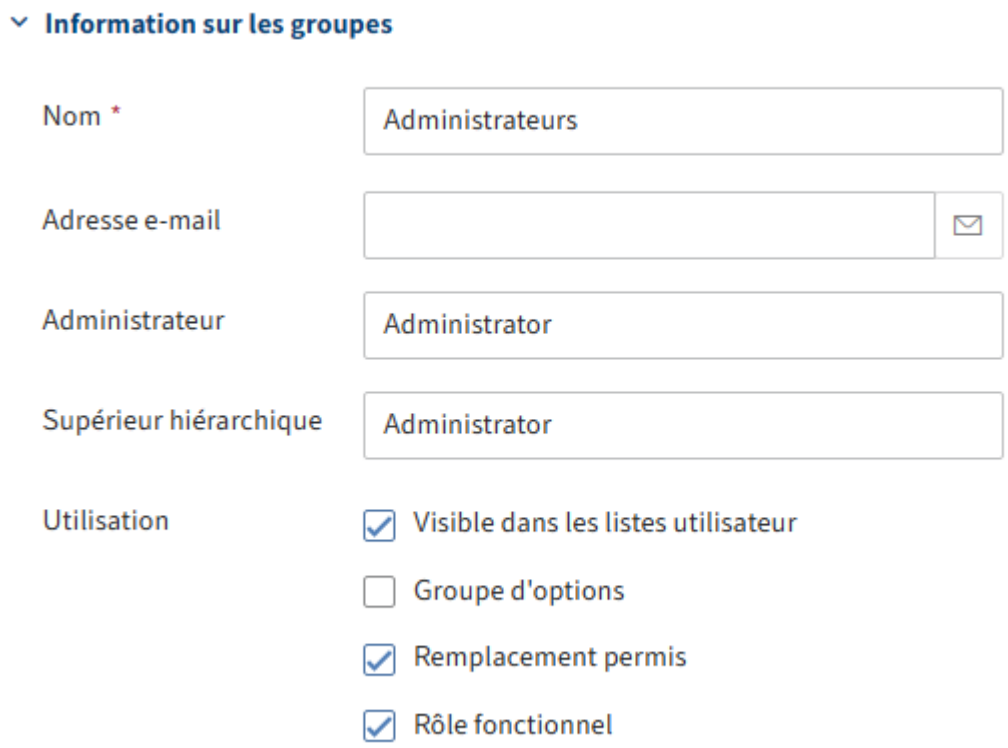
Vous avez créé un nouveau groupe.

Configuration

Déterminer les réglages de base

Dans la section *Réglages de base*, définissez les *Informations de groupe*, *Propriétés* et *Informations* supplémentaires.

Information de groupes



- Nom : champ obligatoire. Peut être modifiée ultérieurement.
- Adresse e-mail : est affichée dans le client dans le profil correspondant et elle pourra être utilisée dans des processus, des formulaires et scripts.
- Administrateur : est rempli automatiquement avec le nom du compte avec lequel le nouveau groupe est créé. Si le compte possède le droit *Administrateur principal*, le champ *Administrateur* est rempli avec le compte *Administrateur*. Peut être modifié ultérieurement. Permet de déterminer qui a le droit de modifier les données de base du groupe en question.
- Supérieur : peut être utilisé dans des processus, formulaires et scripts. Le contenu du champ *Nom* est copié lorsque ce champ reste vide.
- Utilisation :
    - *Visible dans les listes utilisateurs* : si cette option est activée, le groupe apparait dans les listes de sélection dans le client ELO. SI l'option est désactivée, le groupe

continue d'exister dans le client ELO, mais il n'est pas affiché dans les dialogues avec les listes de sélection affichant les utilisateurs ou les groupes.

- *Groupe d'options* : les groupes d'option sont définies pour assigner des *ProfileOpts*. Seuls ces groupes apparaissent dans les dialogues dans lesquels les réglages apparaissent pour d'autres comptes ELO.

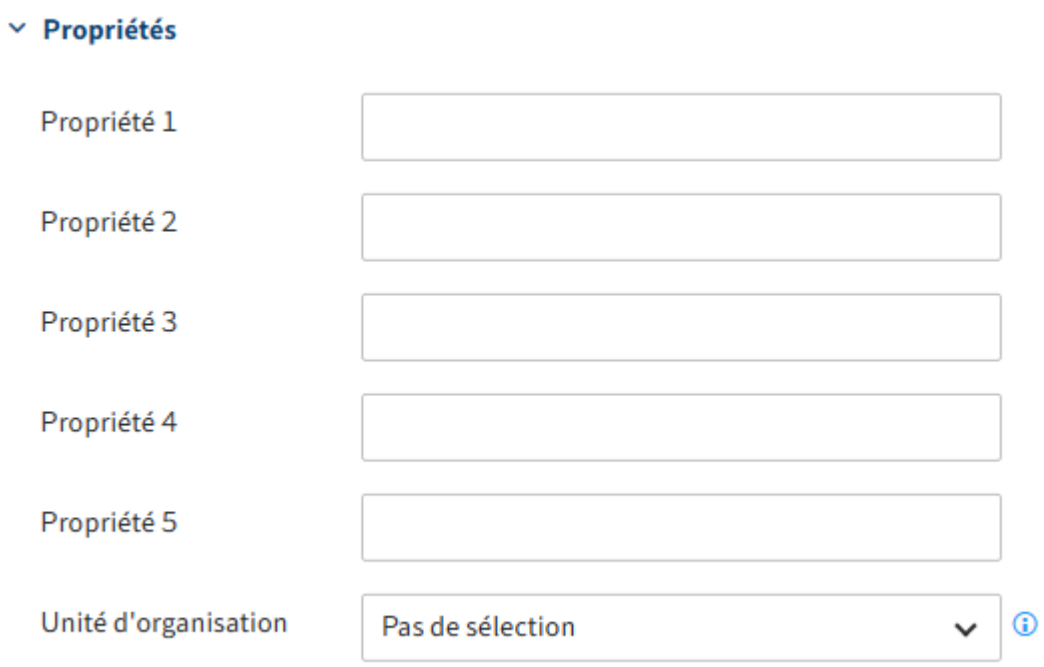
  Vous trouverez des informations au sujet des groupes d'option sous Groupes d'option.

- *Remplacement autorisé* : la répartition des droits peut être dirigée par le biais du module de remplacement. Pour ce qui est des groupes pour lesquels le remplacement est permis, les droits peuvent être transférés aux remplaçants.

- *Rôle fonctionnel* : lorsque cette option est activée, les membres du groupe obtiennent une interrogation lors de l'authentification, à savoir s'ils souhaitent endosser le *rôle fonctionnel* pour cette session.

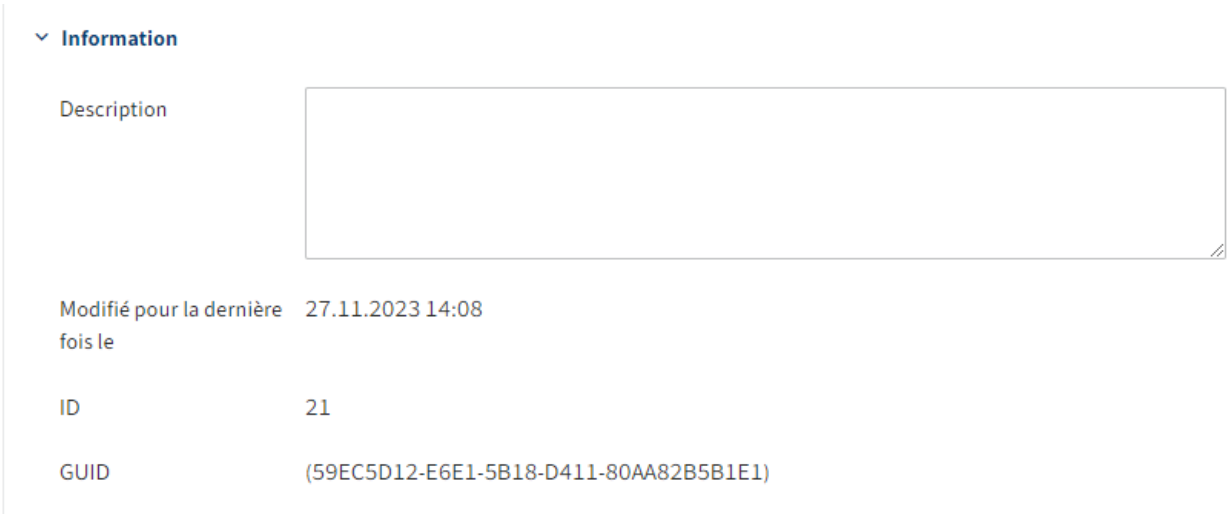
  Cela est recommandé lorsqu'un utilisateur doit remplir plusieurs rôles dans ELO, qui requièrent différentes autorisations et droits.

Propriétés



- Propriété 1-5 : les informations peuvent être analysées via des scripts.
- Unité d'organisation : vous trouverez des informations à ce sujet sous Configuration et administration > Gestion utilisateurs > Autres configurations > Unités d'organisation.

Information



- Description : l'entrée ne doit pas faire plus de 250 caractères.
- Modifié récemment : s'actualise automatiquement
- ID : Jede Gruppe erhält automatisch eine ID. Die ID kann zur Ansprache der Gruppe bei anderen Funktionen verwendet werden.
- GUID : chaque groupe obtient automatiquement un GUID. Le GUID peut être utilisé pour s'adresser au groupe pour d'autres fonctions.

Groupes d'options

En règle générale, ce sont les options individuelles qui sont utilisées pour un compte. S'il n'existe pas d'options personnelles, les options sont utilisées pour les groupes d'option. Lorsque celles-ci n'ont pas été définies, c'est le réglage d'option du groupe *Tout le monde* qui est utilisé. Si rien n'a été défini ici, il existe une valeur standard ELO (*company default setting* ou standard client).

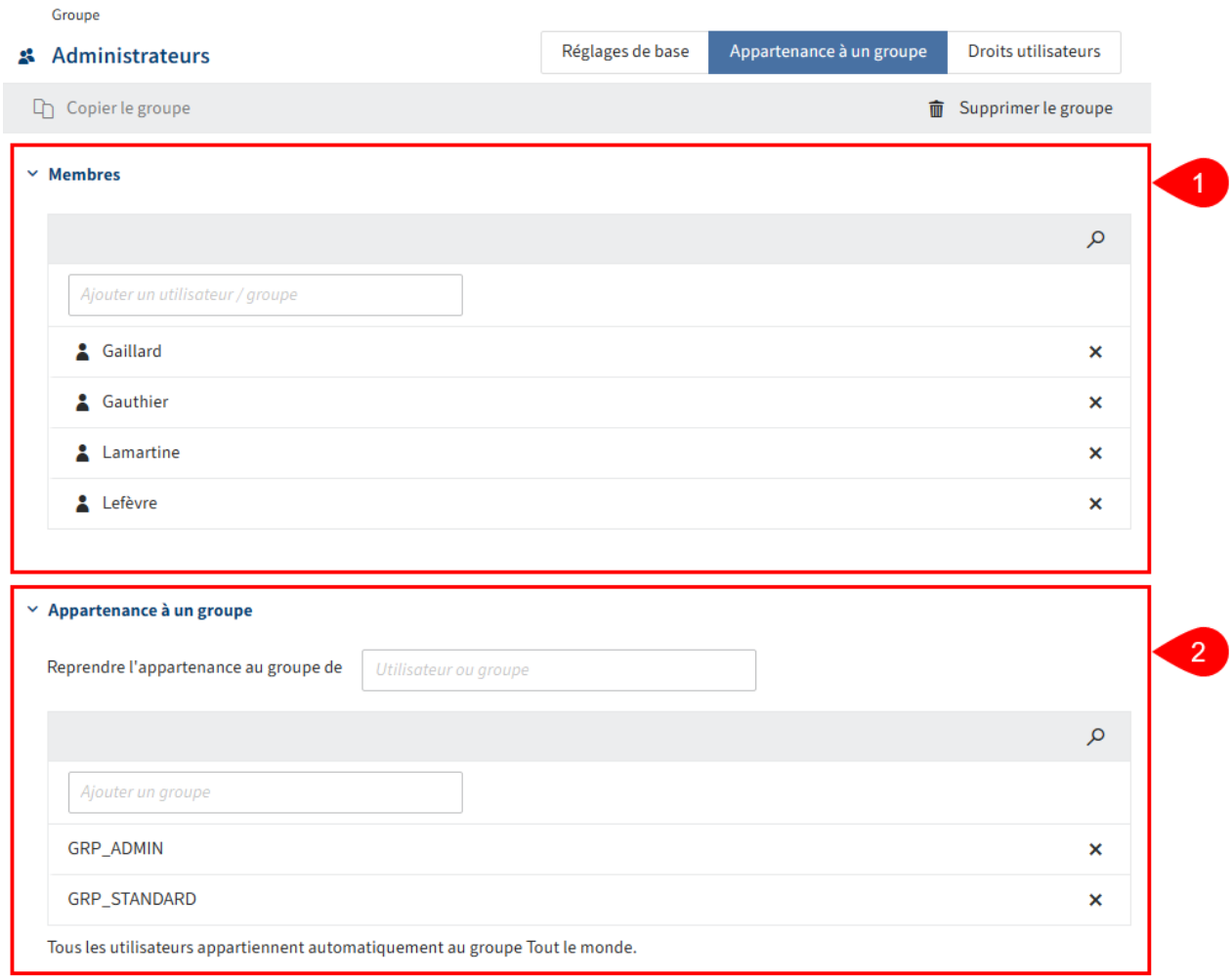
Ces groupes vous permettent de contrôler qui peut accéder à quelle fonction et dans quel contexte.

Vous pouvez définir quel utilisateur ne peut utiliser certaines fonctions que via la touche droite de la souris, ou via les symboles du ruban, ou via les deux, ou pas du tout. Les scripts et leur exécution peuvent également être dirigés de façon distincte pour chaque groupe d'option.

Cela peut être particulièrement pratique pour les postes de travail ELO ayant à effectuer des tâches bien précises. Les postes de travail ELO sont mieux structurés et ils n'utilisent que les fonctions dont ils ont besoin.

> **Remarque**
>
> Un compte ELO ne devrait se trouver que dans un groupe d'options. Les appartenances à plusieurs groupes d'options peuvent avoir pour effet qu'il y ait des interférences entre les différents réglages.

Définir l'appartenance à un groupe



1 Membres : ajouter des utilisateurs ou des groupes existants en tant que membres.

2 Appartenance à un groupe : le champ Copier l'appartenance à un groupe de vous permet d'adopter une appartenance à un groupe d'autres groupes ou utilisateurs.

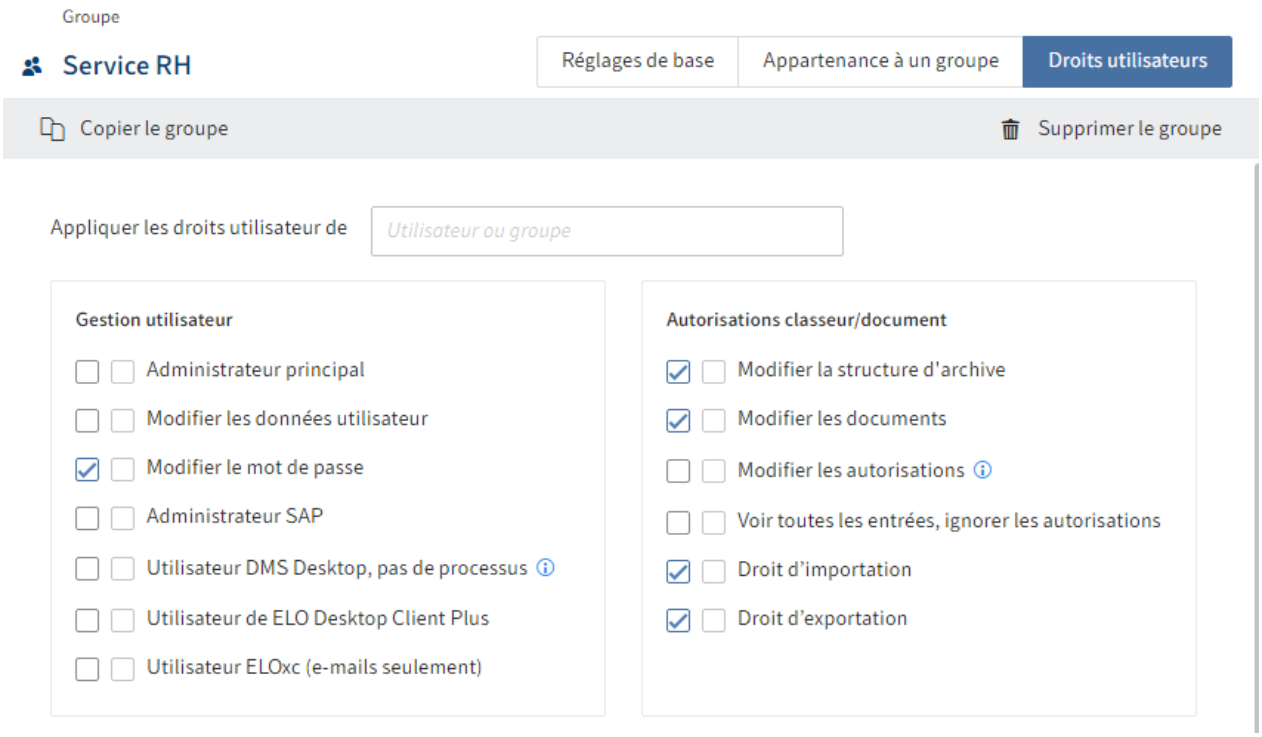
> **Information**

Les groupes peuvent être ajoutés à d'autres groupes. De cette manière, il est possible de réaliser des combinaisons complexes de réglages de droits.

Information

Tapez un espace dans un des champs de saisie pour faire afficher l'intégralité de la liste des utilisateurs et groupes existants.

Assigner les droits utilisateurs



Il existe trois possibilités pour l'attribution des droits utilisateurs :

- Transmission

  Vous trouverez d'autres informations à ce sujet sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Leg de droits

- Assignation manuelle

  Vous trouverez d'autres informations à ce sujet sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Droits utilisateur

- Copier les droits utilisateur d'un autre groupe ou d'un utilisateur

Information

Dans l'idéal, tous les droits seront légués via des groupes. Cela permet de simplifier considérablement l'assignation et l'administration des droits.

Autres configurations

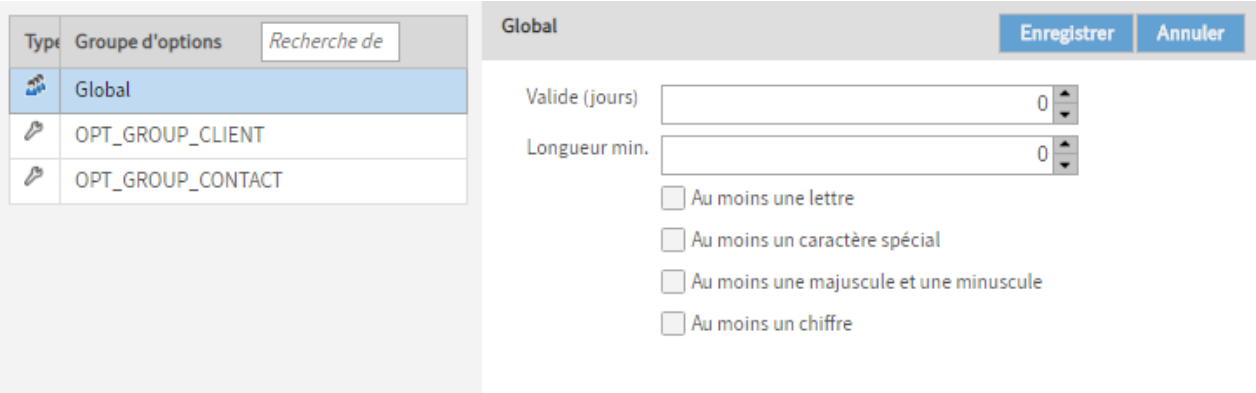
Introduction

D'autres configurations pour l'administration de la gestion des utilisateurs.

- Définir les Règles des mots de passe
- Verrouiller l'accès
- Unités d'organisation

Règles pour les mots de passe

Dans la section *Règles pour les mots de passe*, vous pouvez définir les règles pour la sécurité du mot de passe.

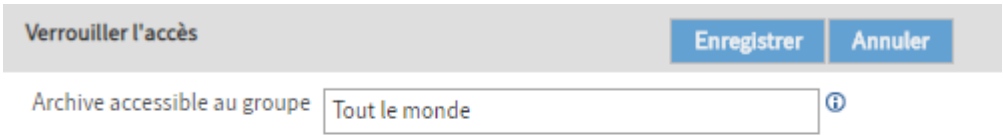


Validité (en jours) : vous pouvez définir la durée de validité du mot de passe.

Longueur min. : vous pouvez définir la longueur min. pour les mots de passe dans ELO.

> **Information**
>
> Plus vous utilisez de caractères spéciaux, plus le mot de passe est sûr. Vous pouvez déterminer quels caractères doivent être utilisés dans le mot de passe.

Verrouiller l'accès



Le point de menu *Verrouiller l'accès* (*Autres* > *Verrouiller l'accès* vous permet de déterminer que seuls les membres du groupe sélectionné ont accès à ELO.

Archive accessible au groupe : dès que vous commencez à entrer quelque chose dans ce champ, ELO vous propose des groupes appropriés. Veuillez sélectionner un groupe et confirmez votre sélection avec *Enregistrer*. Le répertoire correspondant ne sera accessible que pour les membres de ce groupe.

Remarque

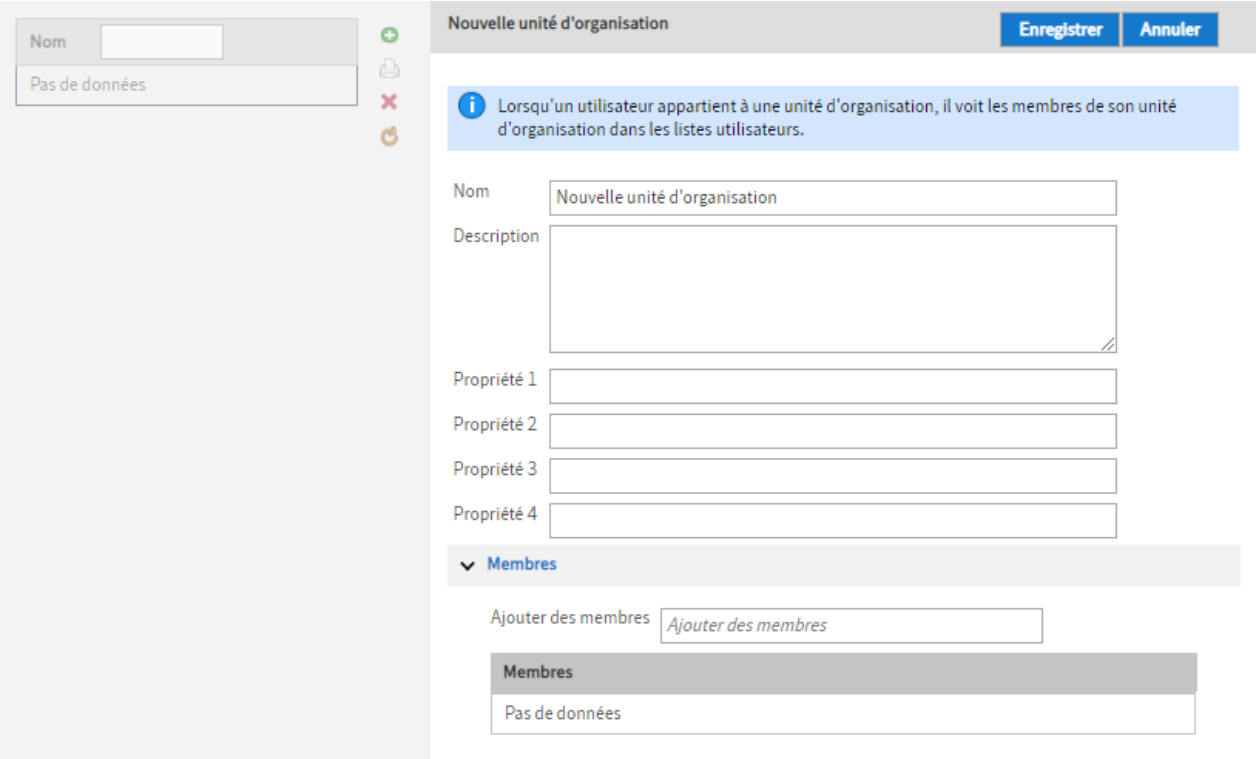
Une authentification de comptes qui disposent du droit utilisateur *Administrateur principal* est possible à tout moment. Les utilisateurs qui sont déjà authentifiés peuvent utiliser ELO jusqu'à leur déconnexion.

Information

Pour valider le répertoire pour tous les comptes, utilisez le groupe *Tout le monde*.

Unités d'organisation

Les unités d'organisation s'ouvrent dans la console d'administration ELO via *Réglages systèmes > Unités d'organisation*.



Les unités d'organisation servent à gérer et structurer les comptes.

Les membres d'une unité d'organisation voient seulement les membres se trouvant dans leur unité d'organisation.

Cela peut être très utile dans les grandes sociétés, par exemple quand les différentes dépendances ne travaillent pas directement ensemble. Un compte ou un groupe ne peut appartenir qu'à une seule unité d'organisation. L'appartenance à une unité d'organisation ne peut être léguée que par le biais de groupes.

> **Information**
>
> Remarque : différentes unités d'organisation ne sont pas en mesure de gérer des comptes du même nom.
>
> Exemple : il n'est pas sensé que trois différentes unités d'organisation contiennent tous le compte *Administrateur*.

Droits et autorisations dans ELO

Introduction

Cette documentation aborde le sujet des droits et de leur assignation dans ELO.

L'assignation des droits permet de déterminer quelles actions peuvent être effectuées dans ELO. Les droits sont assignés dans la console d'administration ELO.

Les droits valent dans ELO. De plus, il existe des autorisations qui valent pour les entrées et éléments individuels dans ELO. La combinaison d'autorisations et de droits a donc un effet sur les actions ayant le droit d'être effectuées sur une entrée ou un élément.

Exemples :

1. Vous possédez le droit utilisateur *Supprimer les documents*, qui vous permet de supprimer des documents dans ELO. Vous ne disposez que de l'autorisation particulière *Voir (R)* pour un document particulier. Vous ne pouvez pas supprimer ce document malgré le droit général, étant donné que vous ne disposez pas de l'autorisation pour supprimer exactement ce document.

2. Vous avez les autorisations *Voir (R)* et *Supprimer (D)* pour un document particulier. Toutefois, vous n'avez pas le droit utilisateur *Supprimer les documents*. Vous ne pouvez pas supprimer ce document en raison des autorisations définies, étant donné que vous ne possédez pas le droit, et que vous n'avez pas le droit de supprimer de documents dans le système.

Vous trouverez d'autres informations dans les paragraphes suivants :

- Droits utilisateurs
- Transmission de droits
- Attribution des droits dans les ELO Spaces
- Configuration

Thème apparenté

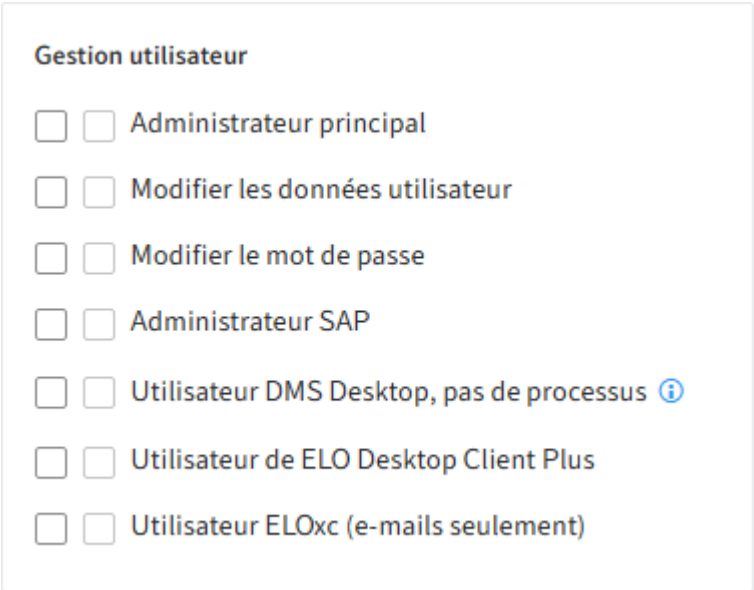
Autorisations dans ELO : grâce à l'assignation des autorisations, vous pouvez définir qui a le droit d'exécuter quelles actions sur une entrée ou un élément précis dans ELO.Vous trouverez d'autres informations au sujet des autorisations dans ELO sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Leg de droits

Droits utilisateurs

Les droits utilisateur peuvent être gérés dans la configuration des Utilisateurs et des Groupes.

> **Information**
>
> Dans l'idéal, tous les droits seront légués via des groupes. Cela permet de simplifier considérablement l'assignation et l'administration des droits.

Droits sur la gestion des utilisateurs



Administrateur principal (FLAG_ADMIN)

Ce droit est requis pour effectuer des réglages globaux.

Si vous possédez le droit *Administrateur principal*, vous pouvez visualiser tous les utilisateurs et groupes, même si l'option *Visible dans les listes utilisateurs* est désactivée pour ceux-ci. Si vous possédez en plus le droit *Modifier les données utilisateur*, vous pouvez gérer tous les utilisateurs et groupes.

Le droit *Administrateur principal* permet de modifier le niveau d'archive supérieur : pour modifier les autorisations et options des niveaux d'archive supérieur, il faut ouvrir le dialogue *Définir les autorisations*, ce qui est est seulement possible avec le droit *Administrateur principal*. Pour réellement modifier les autorisations, il vous faut le droit *Modifier les autorisations*, les deux droits sont donc requis dans ce cas.

Avec le droit *Administrateur principal*, vous avez le droit d'effectuer les actions suivantes dans ELO :

- Supprimer définitivement les entrées, même lorsque vous ne possédez pas les droits *Supprimer les classeurs*, *Supprimer les documents*, *Supprimer les documents non-modifiables* et *Supprimer les versions*
-

L'administrateur peut supprimer un verrouillage pour toutes les entrées; et non seulement pour les entrées qu'il a verrouillé lui-même.
- Mettre en place un remplaçant pour tous les utilisateurs
- Gérer les affichages et profils d'affichage pour tous les utilisateurs.
- Supprimer des masques
- Authentification au mode administrateur ou pour une archive fermée

Vous trouverez d'autres informations sous Droits dans ELO > Configuration > Droits nécessaires pour les sections de la console d'administration ELO.

Modifier les données utilisateur (FLAG_SUBADMIN)

Avec le droit *Modifier les données utilisateur*, vous avez le droit d'effectuer les actions suivantes dans ELO :

- Créer des utilisateurs et groupes Les groupes et d'autres utilisateurs ne peuvent être dotés que des mêmes droits (ou de moins de droits)
- Administrer les utilisateurs et groupes, lorsque vous possédez en plus le droit *Administrateur principal* ou que vous êtes défini comme *Administrateur* de l'utilisateur ou du groupe correspondant. Lorsqu'un groupe est entré dans le champ *Administrateur*, tous les membres de ce groupe peuvent administrer l'utilisateur ou le groupe correspondant, lorsque le groupe possède en plus le droit *Administrateur principal*.
- Vous ne pouvez assigner que des groupes dans lesquels vous êtes entré comme *Administrateur* ou si vous possédez en plus le droit *Administrateur principal*.
- Gérer les propres données utilisateur, lorsque vous êtes défini en tant qu' *Administrateur* dans la gestion des utilisateurs ou si vous possédez en plus le droit *Administrateur principal*.
- Dans le client Java, les *Règles de remplacement pour d'autres* : permettent de définir les règles de remplacement pour les utilisateurs qui s'administrent eux-mêmes, même si ces utilisateurs ne sont pas *Visibles dans les listes utilisateurs*.

> **Information**
>
> Seuls les utilisateurs possédant les droits *Administrateur principal* et *Modifier les données utilisateur* peuvent voir et administrer tous les utilisateurs.

Modifier le mot de passe (FLAG_CHANGEPW)

Ce droit permet de modifier le propre mot de passe pour l'authentification dans le système.

Administrateur SAP (FLAG_SAPADMIN)

Ce droit permet de créer une interface entre ELO et SAP, grâce à la ELO Suite for SAP ArchiveLink® et permet de gérer le masque de dépôt correspondant. Le masque de dépôt pour les documents gérés par SAP est visible pour tous, mais il ne peut être modifié que lorsque l'on possède ce droit.

Utilisateur DMS Desktop, pas de processus (FLAG2_IS_DMS_DESKTOP_USER)

Avec cette option, les fonctions de processus ne sont pas disponibles. Les fonctions suivantes sont concernées :

- Processus ad-hoc
- Prolonger la durée du processus
- Aperçu des processus
- Transmettre le processus
- Accepter
- Afficher le processus
- Déléguer le processus
- Démarrer le processus
- Traiter le processus
- Rendre le processus
- Ajourner le processus
- Processus liés à l'entrée
- Modifier les modèles de processus
- Annuler l'ajournement

> **Remarque**
>
> Ce droit n'est pas un droit, mais plutôt une restriction et écrase tous les autres droits qui existent dans le processus. Lorsque ce droti est défini, il ne peut plus utiliser les fonctions et rôles qui concernent les processus, que les droits soient définis directement ou hérités. Les tâches de processus qui ont également été assignées ne peuvent pas être modifiées. Il en est ainsi parce qu'il n'y a pas de processus dans ELO DMS Desktop.

Utilisateur ELO Desktop Client Plus (FLAG2_DESKTOP_CLIENT_PLUS)

Ce droit ouvre le client ELO Desktop au mode avancé, avec quelques fonctionnalités du mode des tâches et du mode de représentation du client intégral.

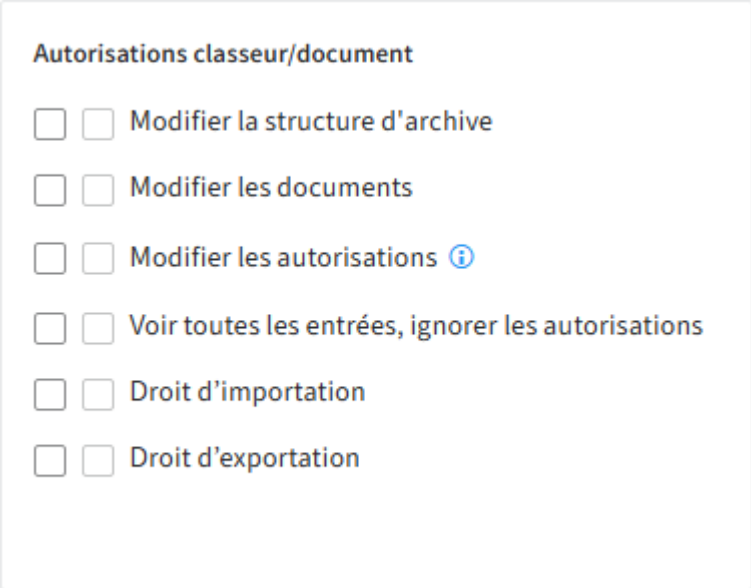
> **Remarque**
>
> Ce droit restreint les fonctions.

Utilisateur client ELOxc, seulement les e-mails (FLAG2_LIMITED_CLIENT)

Ce droit ouvre le Client for Microsoft Outlook dans le mode ELOxc for Microsoft EWS, limité aux formats de fichier (EML, MSG und VCF), qui peuvent être ouverts par Microsoft Outlook. Les autres formats ne sont pas disponibles.

> **Remarque**
>
> Ce droit restreint les fonctions.

Droits pour les classeurs/documents



Modifier les classeurs (FLAG_EDITSTRUCTURE)

Ce droit permet le traitement et la création des structures dans les classeurs.

Modifier les documents (FLAG_EDITDOCS)

Ce droit permet de modifier des documents. Il s'agit de :

- Charger des nouvelles versions
- Check-in et check-out
- Ajouter des fichiers
- Documents à partir d'un modèle
- Ajouter et supprimer des fichiers associés.
- Enregistrer dans le plein texte
- Supprimer du plein texte
- Créer une signature

Les métadonnées ne peuvent pas peut être modifiées à condition de posséder le droit correspondant. Sans ce droit, les métadonnées s'ouvrent en lecture seule.

Modifier les autorisations (FLAG_EDITACL)

Ce droit permet le traitement des autorisations des entrées (documents et classeurs) dans ELO.

> **Information**
>
> Pour modifier les autorisations des entrées, l'on a besoin du droit *Modifier les classeurs* ou *Modifier les documents*. De plus, l'autorisation *Définir les autorisations* (P) est requise pour les différentes entrées.

Lors du dépôt dans le client, l'utilisateur a la possibilité de configurer les droits, étant donné qu'il possède tous les droits sur le document. Le droit utilisateur se réfère au traitement ultérieur des autorisations.

Ce droit ne concerne pas les réglages de droits dans la console d'administration ELO ou dans la configuration du client Java ELO. Si l'utilisateur peut traiter les tampons, masques etc., il est également en mesure de modifier les autorisations sans que ce droit utilisateur soit vérifié.

Voir toutes les entrées, ignorer les autorisations (FLAG_IGNOREACL)

Ce droit signifie que tous les documents et classeurs doivent être affichés, même s'ils sont verrouillés pour le compte correspondant. Il annule toutes les autorisations d'objet existantes. L'utilisateur possédant ce droit possède toutes les autorisations de toutes les entrées ELO.

La seule manière de protéger les comptes des utilisateurs possédant ce droit est de les crypter.

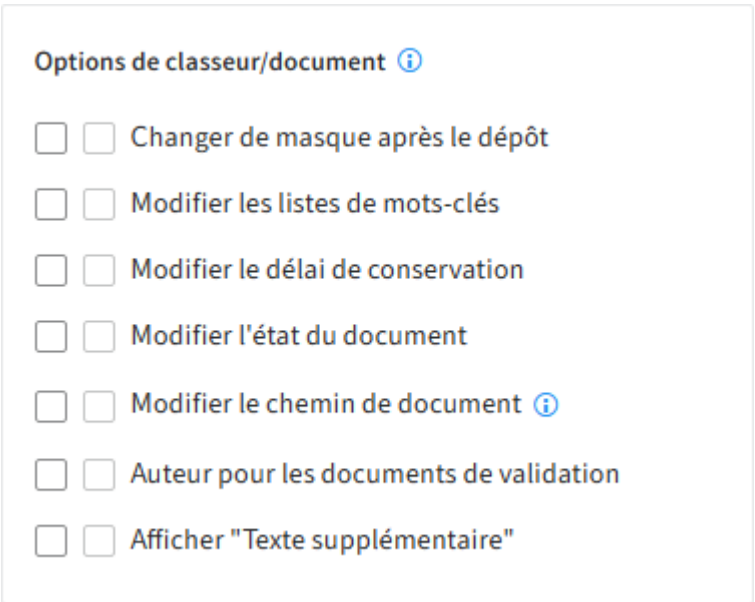
Autorisation d'importation (FLAG_IMPORT)

Ce droit permet l'importation d'un jeu de données dans l'archive. Toutes les données se trouvant dans le jeu de données sont importées, indépendamment des autorisations d'objet. Les données pour lesquelles le compte ne possède pas d'autorisation sont également importées. Ensuite, ces données ne seront pas visibles par le biais de ce compte.

Autorisation d'exportation (FLAG_EXPORT)

Ce droit permet de créer un jeu de données d'exportation. Il ne possède que le droit d'exporter les objets et documents ELO sur lesquels il possède les autorisations correspondantes.

Droits sur les options de classeur/options de document



Information

Les droits de ce groupe (hormis *Modifier le chemin de document*) ne sont que valides lorsque l'utilisateur dispose du droit *Modifier les classeurs* et *Modifier les documents*.

Changer de masque après le dépôt (FLAG_CHANGEMASK)

Ce droit permet d'assigner ultérieurement un document déjà déposé à un autre masque. Il se pourrait cependant que les métadonnées soient perdues. Toutefois, ceci est seulement possible lorsque le droit *Modifier la structure d'archive* ou *Modifier les documents*, est disponible, en fonction de l'entrée.

Modifier la liste des mots-clés (FLAG_EDITSWL)

Ce droit permet de modifier les listes de mots-clés. Il est possible d'ajouter de nouvelles entrées, de les modifier et de les supprimer. Sans ce droit utilisateur, l'on ne peut pas modifier les listes de mots-clés dans la gestion des masques dans la console d'administration, même si l'on possède le droit *Modifier les masques d'indexation*.

Toutefois, ceci est seulement possible lorsque le droit *Modifier les classeurs* ou *Modifier les documents*, est disponible, en fonction de l'entrée.

Modifier le délai de conservation (FLAG_EDITDUEDATE)

Avec ce droit, il est possible de définir et de prolonger le délai de conservation (elle ne peut que être repoussée et non pas avancée). Si le droit n'a pas été défini, le champ correspondant est désactivé dans le dialogue *Métadonnées*.

Toutefois, ceci est seulement possible lorsque le droit *Modifier les classeurs* ou *Modifier les documents*, est disponible, en fonction de l'entrée.

Modifier l'état de document (FLAG_CHANGEREV)

Ce droit permet de définir le statut de document dans le dialogue *Métadonnées* via l'onglet *Options* de documents :

- Pas de contrôle de version
- Contrôle de la version activé
- Pas de modification possible

Toutefois, ceci est seulement possible lorsque le droit *Modifier les documents*, est disponible.

Modifier le chemin de document (FLAG_CHANGEPATH)

Avec ce droit, l'on peut utiliser la liste de sélection pour le chemin de document dans les options. C'est seulement possible pour l'entrée des métadonnées dans la boîte de réception. Si un document a déjà été déposé, cette liste de sélection devient inactive à jamais. Il est possible de déplacer les documents sur un autre chemin ultérieurement avec la fonction *Déplacer les fichiers document* et le droit *Administrateur principal*.

Avec ce droit, il n'est pas possible de créer de nouveaux chemins de document et de modifier leur définition. Pour modifier, créer et assigner les chemins de document, vous avez besoin du droit *Administrateur principal*.

Auteur pour les documents de validation (FLAG_AUTHOR)

Ce droit permet d'activer ou de désactiver la case à cocher *Document de validation* et de modifier les documents de validation : l'auteur a la possibilité de modifier les versions antécédentes d'un document. Lors du check-out, s'affiche un dialogue de sélection de toutes les versions de document. L'ancienne version de travail est conservée lors du check-in. La version de travail (= version validée) peut seulement être modifiée par un auteur de documents de validation.

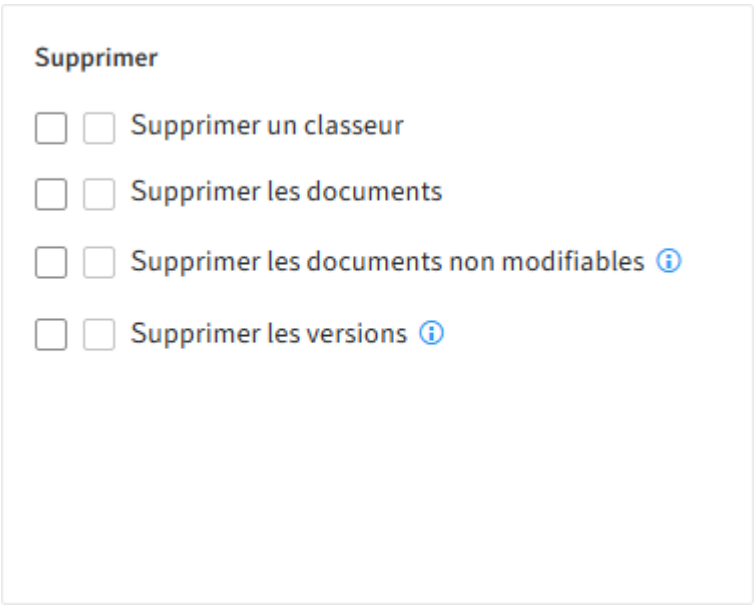
Toutefois, ceci est seulement possible lorsque le droit *Modifier les documents*, est disponible.

Afficher "Texte supplémentaire" (FLAG2_SHOW_EXTRA_INFO)

Ce droit détermine si l'utilisateur doit avoir le droit de voir l'onglet *Informations supplémentaires* dans le dialogue *Métadonnées*.

Toutefois, ceci est seulement possible lorsque le droit *Modifier les classeurs* ou *Modifier les documents*, est disponible, en fonction de l'entrée.

Droits de suppression



Supprimer un classeur (FLAG_DELSTRUC)

Ce droit détermine si un utilisateur a le droit de supprimer des classeurs.

Supprimer des documents (FLAG_DELDOC)

Ce droit détermine si un utilisateur a le droit de supprimer des documents.

Supprimer les documents non modifiables (FLAG_DELREADONLY)

Avec ce droit, un utilisateur peut supprimer les documents possédant le statut de document *Pas de modifications possibles*.

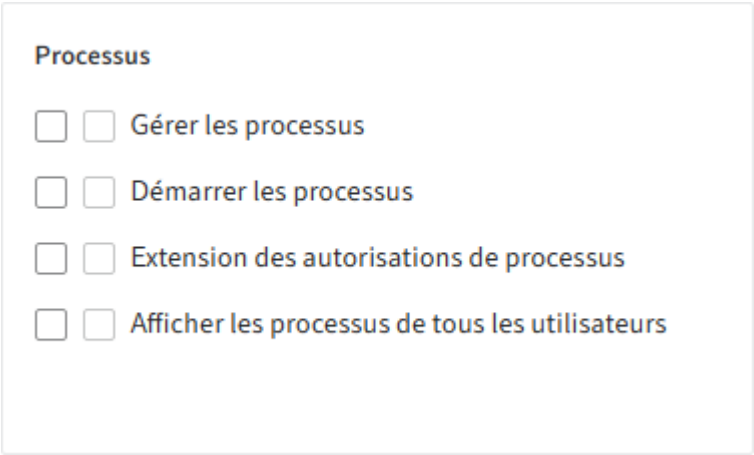
Toutefois, ceci est seulement possible lorsque le droit *Supprimer les documents*, est disponible.

Supprimer les versions (FLAG_DELVERSION)

Ce droit permet de supprimer des versions dans la gestion de version d'un document.

Dans le client Java ELO, l'on peut visualiser les versions de document supprimées dans le dialogue *Version de document*, si la fonction *Afficher les entrées supprimées* est activée.

Droits des processus



Gérer les processus (FLAG_EDITWF)

Le droit de gestion des processus implique :

- Créer les modèles de processus et les formulaires
- Il est possible de terminer prématurément les processus actifs existants.
- Supprimer définitivement les processus clôturés et terminés prématurément
- Modifier les noeuds suivants

Démarrer les processus (FLAG_STARTWF)

Ce droit permet de démarrer des processus. Les fonctions suivantes sont concernées :

- Processus ad-hoc
- Aperçu des processus
- Démarrer le processus
- Processus liés à l'entrée

Il a également besoin de ce droit pour démarrer un processus lors du dépôt d'entrées avec un masque lié à un processus défini. S'il ne détient pas ce droit, il peut déposer les documents avec ce masque, mais le processus n'est pas démarré.

Ce droit est également vérifié pour activer *l'aperçu des processus* et *les processus liés* à l'entrée dans le ruban du client ELO. Ainsi, l'utilisateur peut avoir un aperçu de tous les processus dans lesquels il est impliqué directement ou indirectement.

Extension des autorisations (FLAG2_EXTEND_WORKFLOW_RIGHTS)

Si ce droit est attribué, l'utilisateur obtient un droit de lecture temporaire pour l'entrée se trouvant dans le noeud de processus actif. La lecture du document n'est que possible dans la

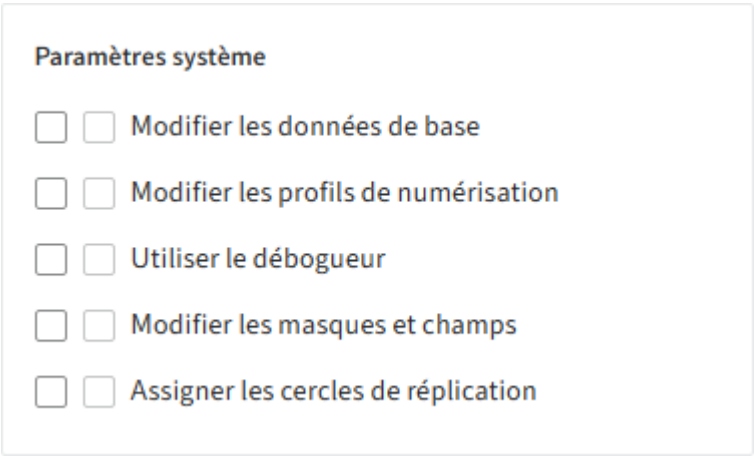
section des tâches, et seulement si le document est adressé à l'utilisateur en question ou au groupe auquel il fait partie. De plus, une entrée dans le tableau *ProfileOpts* de la base de données permet de définir combien d'autres autorisations doivent être assignées de manière temporaire ou permanente.

Ce droit ne peut pas remplacer d'autres droits utilisateurs (cela n'est pas possible même temporairement). Le droit concerne les documents et classeurs, mais non pas les masques.

Afficher les processus de tous les utilisateurs (FLAG2_WF_CONTROLLER)

Le droit permet à un utilisateur de voir tous les processus actifs et non pas seulement les processus dans lesquels l'utilisateur est impliqué.

Droits sur les paramètres système



Modifier les données de base (FLAG_EDITCONFIG)

Avec ce droit, l'utilisateur peut accéder à la gestion des *types d'entrée* (icônes et désignations pour les classeurs et documents), aux *couleurs de l'écriture* et aux *tampons*.

Modifier les profils de numérisation (FLAG_EDITSCAN)

L'activation de cette fonction autorise l'utilisateur à modifier les réglages des paramètres de numérisation et *les profils de numérisation*. Avec le droit *Administrateur principal*, vous avez le droit de modifier et de gérer les *profils et réglages de scanner* pour d'autres comptes.

Utiliser le débogueur (FLAG_EDITSCRIPT)

Dans le client ELO, l'on peut ouvrir le débogueur JavaScript par le biais du raccourci Ctrl+Alt+D si l'on possède ce droit.

> **Information**
>
> Dans ELO, les scripts sont gérés comme les documents. Pour avoir le droit de modifier les scripts, il faut posséder les autorisations correspondantes.

Modifier les masques et champs (FLAG_EDITMASK)

Avec ce droit, il est possible de créer de nouveaux masques et de modifier les masques existants.

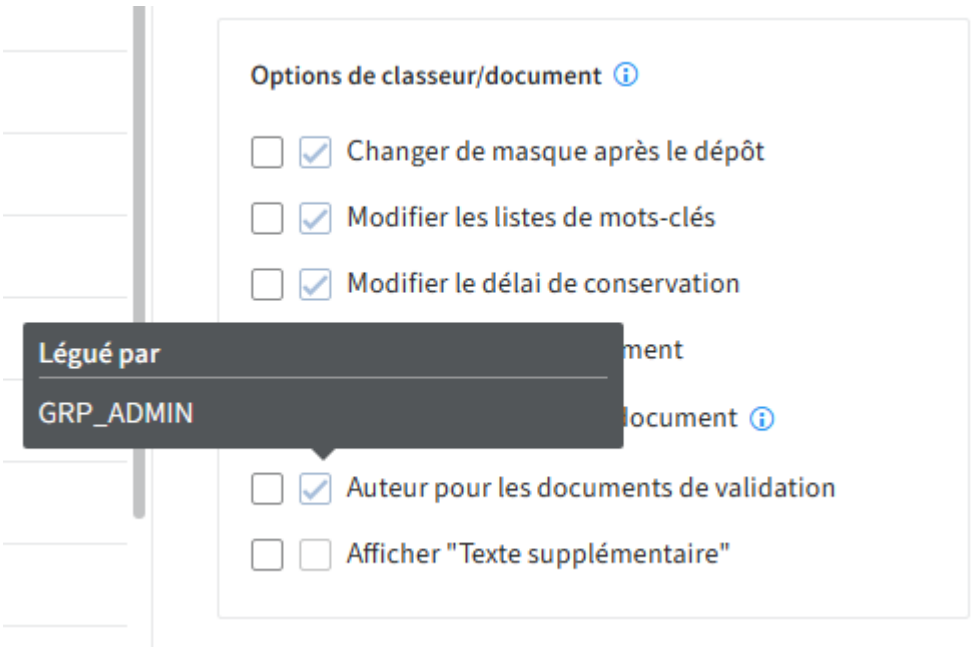
Si les listes de mots-clés doivent être modifiées dans les masques, le droit *Modifier les listes de mots-clés* est également requis.

Assigner les cercles de réplication (FLAG_EDITREPL)

Ce droit est requis pour assigner les données d'archive aux cercles de réplication. Les cercles de réplication sont requis par ELO Replication pour pouvoir déterminer la quantité comparée.

Transmission de droits

Deux boîtes à cocher se trouvent devant les Droits utilisateurs. Les cases à cocher à gauche se réfèrent aux droits individuels du compte ou du groupe. Les cases à cocher à gauche affichent les droits extraits à partir de l'affiliation aux groupes de l'utilisateur. Si vous passez sur la case à cocher de droite avec la souris, une infobulle avec les informations de groupe du droit en question apparaît.



Information

Dans l'idéal, tous les droits seront légués via des groupes. Cela permet de simplifier considérablement l'assignation et l'administration des droits.

Attribution des droits dans les ELO Spaces

Les droits pour les teamspaces et workspaces dans ELO sont déterminés via les rôles assignés.

Teamspace

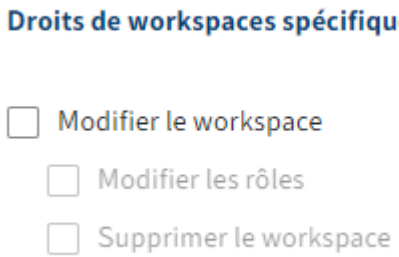
Vous pouvez assigner des droits de teamspace suivants à un rôle :

- Modifier les rôles : modifier et créer les rôles dans le teamspace, indépendamment du fait si le teamspace peut être modifié.
- Modifier le teamspace : apporter des modifications à un teamspace. De plus, il est possible de modifier l'assignation des rôles des membres du teamspace, et d'ajouter de nouveaux membres.
- Supprimer un teamspace : peut seulement être activé lorsque *Modifier le teamspace* est activé.

Vous trouverez d'autres informations au sujet des rôles dans le teamspace sous Packages ELO > Teamspaces ELO > Définir les rôles.

Workspace

Vous pouvez assigner des droits de workspace suivants à un rôle :



- Modifier le workspace : apporter des modifications à un workspace. De plus, il est possible de modifier l'assignation des rôles des membres du workspace, et d'ajouter de nouveaux membres.
- Modifier les rôles : modifier et créer les rôles dans le workspace. Peut seulement être activé lorsque *Modifier le workspace* est activé.
- Supprimer le workspace : peut seulement être activé lorsque *Modifier le workspace* est activé.

Vous trouverez d'autres informations au sujet des rôles dans le workspace sous Packages ELO > Workspaces ELO > Définir les rôles.

Configuration

Droits nécessaires pour les sections de la console d'administration ELO

Paramètres système

Section administratives	Droits
Gestion utilisateurs	Modifier les données utilisateur, administrateur principal Le droit *Administrateur principal* permet d'administrer TOUS les utilisateurs et non seulement ceux pour lesquels vous êtes l'administrateur.
Gestion des groupes	Modifier les groupes, administrateur principal Le droit *Administrateur principal* permet d'administrer TOUS les groupes et non seulement ceux pour lesquels vous êtes l'administrateur.
Unités d'organisation	Administrateur principal Si vous êtes administrateur d'un utilisateur (avec le droit *Modifier les données utilisateur*), vous pouvez assigner cet utilisateur à une unité d'organisation existante, en tant qu'administrateur principal, vous avez accès à la section des unités d'organisation
Masques	Modifier les masques et champs (Le droit *Modifier les listes de mots-clés* est nécessaire pour pouvoir modifier les listes de mots-clés et le droit *Administrateur principal* est requis pour supprimer les masques ou pour enregistrer les données ultérieurement sous forme d'un tableau)
Modèles de champ	Modifier les masques
Masques d'indexation multilingues et Liste de mots-clés	Modifier la liste des mots-clés
Types d'entrée	Modifier les données de base
Chemins de documents	Administrateur principal
Chemins de document standard	Administrateur principal
Cercles de cryptage	Administrateur principal
URL de l'aide en ligne ELO	Administrateur principal
Tampon	Modifier les données de base
URL ELO Forms Services	Administrateur principal
URL ELO Analytics	
Propriétés de l'archive	Administrateur principal
Couleurs de police	Modifier les données de base

Maintenance

Section administratives	Droits
Mode administrateur	Administrateur principal
Options de rapport	Administrateur principal
Supprimer les entrées de rapport	Administrateur principal
Supprimer définitivement	Administrateur principal
Tâches de sauvegarde	Administrateur principal
Règles pour les mots de passe	Administrateur principal
Déplacer les fichiers document	Administrateur principal

Modules serveur

Section administratives	Droits
Services d'automation ELO	Administrateur principal
Profils de sauvegarde	Administrateur principal
Service plein texte	Administrateur principal
Créer un mot de passe	Administrateur principal
ELO Transport	Administrateur principal
Fichiers de configuration	Administrateur principal
Créateur de formulaire	Gérer les processus
ELOxc	*Pas de vérification dans la console d'administration ELO La console ELOxc effectue la vérification.*

Informations système

Section administratives	Droits
Classeur d'administration	Administrateur principal
Informations serveur	Administrateur principal
Utilisateurs authentifiés	Administrateur principal
Statistique	Administrateur principal
Aperçu des licences	Administrateur principal
Informations relatives à la licence	Administrateur principal
Fichiers journaux	Administrateur principal
Monitoring	Administrateur principal
Vérifier les sommes de contrôle	Administrateur principal

Autres

Section administratives	Droits
Importation LDAP	Administrateur principal

Section administratives	Droits
Verrouiller l'accès	Administrateur principal

Cryptage de documents

Dans les systèmes, il existe une méthode pour crypter les documents. Ces documents sont cryptés au niveau du système d'exploitation, un mot de passe est requis. Ces mots de passe sont donc parfaitement protégés d'une éventuelle lecture par des personnes non autorisées, même dans le cadre d'une sauvegarde.

Dans ELO, les documents peuvent être cryptés par le biais des réglages autorisations ACL, en plus de ce cryptage opérant au niveau du système d'exploitation. Ainsi, les documents sont également cryptés pour les administrateurs.

Dans ELO, le verrouillage se fait avec AES-256 (Advanced Encryption Standard), une méthode de cryptage symétrique qui travaille avec un cryptage en bloc. Plus de 16 cercles de verrouillage sont disponibles. Le cryptage et le décryptage se font du côté du serveur.

Les documents ayant déjà été cryptés restent dans l'ancien mode de cryptage. Les deux procédures de cryptage sont marquées dans la base de données, elles sont utilisées en parallèle dans un mode de comptabilité.

Eine cryptage avec les fonctions ELO n'est que possible lors du passage d'un document dans l'archive. Les documents placés dans la boîte de réception ne sont pas cryptés, jusqu'à leur passage dans l'archive. Un cryptage ultérieur de documents se trouvant dans ELO n'est pas possible avec les fonctions ELO et n'est pas sensé, étant donné que les documents se trouvent sur un chemin de réflexion dès qu'ils sont dans l'archive, ainsi que sur des médias en lecture seule et sur différents systèmes de sauvegarde.

Le cryptage peut seulement être effectué par les utilisateurs possédant le droit *Administrateur principal*. Ensuite, tous les utilisateurs peuvent utiliser le cryptage. Il suffit de connaître le cercle de cryptage et le mot de passe. Un cercle de cryptage n'est pas obligatoirement lié à une personne bien précise, il bien également être utilisé pour les groupes.

Les documents cryptés avec AES-256 peuvent être enregistrés dans le plein texte. Pour ceci, un utilisateur système doit être créé; celui-ci gère l'accès aux documents cryptés. Les documents cryptés peuvent, mais ne doivent pas être pris en compte dans la base de données plein texte.

Il faut faire attention de ne pas confondre les cercles de cryptage avec les clés qui ne feront font plus partie des fonctions à partir de la version 10.

Vous trouverez d'autres informations au sujet du cryptage sous Configuration et administration > Administration système > Classeurs & documents > Verschlüsselungskreise.

Autorisations dans ELO

Introduction

Dans ELO, les autorisations sont assignées pour chaque entrée et chaque élément. Cela vous permet de définir qui a le droit d'exécuter quelles actions sur une entrée ou un élément précis dans ELO. Ces autorisations sont assignées dans les métadonnées dans l'onglet *Autorisations*.

Il s'agit des autorisations suivantes :

- R (Read)
- W (Write)
- D (Delete)
- E (Edit)
- L (List)
- P (Permissions)

Les autorisations valent pour les entrées et éléments individuels dans ELO. Les droits valent dans ELO. La combinaison d'autorisations et de droits a donc un effet sur les actions ayant le droit d'être effectuées sur une entrée ou un élément.

Exemples :

1. Vous possédez le droit utilisateur *Supprimer les documents*, qui vous permet de supprimer des documents dans ELO. Vous ne disposez que de l'autorisation particulière *Voir (R)* pour un document particulier. Vous ne pouvez pas supprimer ce document malgré le droit général, étant donné que vous ne disposez pas de l'autorisation pour supprimer exactement ce document.

2. Vous avez les autorisations *Voir (R)* et *Supprimer (D)* pour un document particulier. Toutefois, vous n'avez pas le droit utilisateur *Supprimer les documents*. Vous ne pouvez pas supprimer ce document en raison des autorisations définies, étant donné que vous ne possédez pas le droit, et que vous n'avez pas le droit de supprimer de documents dans le système.

Vous trouverez d'autres informations au sujet des autorisations dans les paragraphes suivants :

- Autorisations générales
- Autres autorisations

Thème apparenté

Droits dans ELO : l'assignation des droits utilisateur permet de déterminer quelles actions ont le droit d'être exécutées dans ELO.Vous trouverez d'autres informations au sujet des droits dans ELO sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Leg de droits

Autorisations générales

Les autorisations pour les entrées et éléments dans ELO diffèrent selon le contexte.

Vous trouverez les autorisations pour les différentes entrées et éléments dans les sections suivantes :

- Documents
- Classeur
- Notes
- Remarques (par exemple tampons, notes)
- Masques
- Modèles de processus
- Processus
- ELO Spaces

Autorisation	Description
Voir (R)	Voir les documents et métadonnées, ajouter des remarques et notes
Modifier les métadonnées (W)	
Supprimer (D)	Marquer le document comme étant supprimé. Seules les personnes avec droits administratifs peuvent supprimer définitivement des documents. Vous trouverez des informations à ce sujet sous Configuration et administration > Administration système > Classeurs & documents > Supprimer et retirer.
Modifier (E)	Modifier les documents, par exemple check-in, check-out, charger une nouvelle version, modifier la version de travail
<modifier la liste> (L)	N'a pas d'effet sur les documents
Définir les autorisations (P)	Modifier les autorisations (définir, modifier, supprimer)

Autorisation	Description
Voir (R)	Voir les classeurs et métadonnées, ajouter des notes
Modifier les métadonnées (W)	
Supprimer (D)	Marquer les classeurs comme étant supprimés, même si des sous-entrées ont le droit d'être supprimées ou que le classeur est vide. Seuls les utilisateurs avec droits administratifs peuvent supprimer définitivement des documents. Vous trouverez des informations à ce sujet sous Configuration et administration > Administration système > Classeurs & documents > Supprimer et retirer.
<Modifier> (E)	N'a pas d'effet sur les classeurs, mais est important pour la transmission des autorisations aux documents placés dans les classeurs.

Autorisation	Description
Modifier la liste (L)	Modifier le contenu, par exemple y créer des documents, les déplacer, les copier ou les retirer, ajouter ou supprimer une référence.
Définir les autorisations (P)	Modifier les autorisations (définir, modifier, supprimer)

Notes

Il existe trois types de notes.

Note générale

Tous les utilisateur qui possèdent l'autorisation *Voir* pour l'entrée, peuvent créer et voir ces notes. Lorsque l'on possède uniquement l'autorisation *Voir* pour l'entrée, l'on ne peut modifier et supprimer que les notes générales que l'on a créé soi-même. Lorsque l'on possède également l'autorisation *Modifier les métadonnées* pour l'entrée, on peut modifier et supprimer toutes les notes.

Note personnelle

Tous les utilisateur qui possèdent l'autorisation *Voir* pour l'entrée, peuvent créer, modifier et supprimer ces notes pour soi-même. Cet utilisateur sera le seul à voir les notes.

> **Information**
>
> Pour ce qui est des autorisations, les remarques sans texte et avec texte ne divergent que pour ce qui est de l'autorisation W (Write).
>
> Les administrateurs principaux ne peuvent pas voir les notes personnelles des autres utilisateurs.

Note permanente

Tous les utilisateur qui possèdent l'autorisation *Voir* pour l'entrée, peuvent créer et voir ces notes. Il n'est pas possible de modifier ou de supprimer des notes permanentes ultérieurement.

> **Remarque**
>
> Les administrateurs principaux ne peuvent pas modifier ou supprimer des notes permanentes ultérieurement.

Remarques

Il existe des remarques avec et sans texte.

Les remarques avec texte désignent les posts-its, les notes de texte, les tampons. Les remarques sont texte sont le marqueur main levée, le marquage de rectangle, le marqueur horizontal, l'outil pour barrer un contenu, le noircissement et le tampon image.

Information

Etant donné que les propriétés de tampon diffèrent un peu des autres remarques, celles-ci sont présentées à part.

Le tableau suivant vaut pour les remarques présentées ci-dessus (à part les tampons) :

Autorisation	Description
Voir (R)	Créer des remarques, modifier et supprimer les remarques créés soi-même
Modifier (W)	Remarques avec texte : modifier le texte et le formater, noter la position, mémoriser la position, modifier la taille; Remarques sans texte : modifier les propriétés (couleur, épaisseur du stylo)
Supprimer (D)	
Déplacer (E)	Modifier la position de la remarque sur le document
<modifier la liste> (L)	N'a pas d'effet sur les remarques b
Définir les autorisations (P)	Modifier les autorisations

Information

Information Pour ce qui est des autorisations, les remarques sans texte et avec texte ne divergent que pour ce qui est de l'autorisation *W (Write)*.

Tampon

Nous faisons une différenciation entre le tampon en tant qu'outil et le tampon en tant que cachet apposé sur un document.

Outil 'Tampon'

Avec ProfileOpts, l'outil *Tampon* est défini pour un utilisateur précis, un groupe d'options ou de manière globale, via *ProfileOpts*. Les tampons peuvent être créés et gérés dans la console d'administration ELO et dans le client Java ELO. Dans le client Java ELO, il est seulement possible de configurer ses propres tampons. Les tampons définis sont affichés dans la liste des tampons des utilisateurs correspondants. Pour qu'un utilisateur puisse utiliser l'outil *Tampon*, au moins au tampon doit lui être assigné par les administrateurs. Sinon, celui-ci ne pourra pas définir de tampon pour lui-même dans le client Java ELO.

Lorsqu'un utilisateur crée un tampon dans le client Java ELO, ce tampon est affiché dans la liste des tampons de l'utilisateur et il ne peut être utilisé que par lui-même. Les tampons créés par l'utilisateur peuvent être gérés par lui-même dans le client Java avec l'outil *Tampon* et par l'administrateur dans la console d'administration ELO. Pour configurer des tampons spécifiques aux utilisateurs ou aux groupes dans la console d'administration ELO, l'administrateur doit sélectionner l'utilisateur ou le groupe correspondant via le bouton *Sélectionner un utilisateur*. Par défaut, le groupe *Tout le monde* est sélectionné.

Empreinte de tampon

Autorisation	Description
Voir (V)	voir le tampon sur le document, mémoriser la position
Modifier (M)	Modifier la taille
Supprimer (D)	
Déplacer (E)	Modifier la position
<modifier la liste> (L)	N'a pas de répercussion sur le tampon
Définir les autorisations (P)	Modifier les autorisations

> **Information**
>
> Pour un tampon appliqué, il faut prendre en considération les même autorisations que lorsqu'il est appliqué. Les autorisations modifiées ultérieurement n'ont pas d'effet sur les tampons déjà apposés, mais seulement sur ceux qui sont nouvellement apposés après la modification.

Masques et champs

Masques

Les autorisations pour les masques peuvent seulement être définies dans la console d'administration ELO.

Autorisation	Description
Voir les métadonnées (R)	Visualiser les masques dans le dialogue *Métadonnées*, visualiser les métadonnées en mode lecture seule.
Modifier les métadonnées (W)	Dépôt des entrées et saisir des métadonnées (aussi comme premier dépôt). Si vous ne possédez pas l'autorisation *W* principale du masque, vous ne pouvez pas modifier les métadonnées des entrées. Même si vous possédez l'autorisation *W* pour l'entrée, le dialogue s'ouvre en mode lecture seule. Pour modifier ensuite les métadonnées d'une entrée déposée, il vous faut en plus l'autorisation *W* sur l'entrée.
Supprimer le masque (D)	Cette autorisation n'est pas vérifiée. Pour pouvoir supprimer des masques dans la console d'administration ELO, vous devez posséder le droit utilisateur *Administrateur principal*.
Modifier le masque (E)	Cette autorisation n'est pas vérifiée.

Champs

La *représentation* des champs permet de déterminer si le champ peut être rempli manuellement (*Accès normal*), s'il ne doit être que visible (*Non éditable*) ou s'il ne doit pas être visible sur l'interface utilisateur (*Invisible)*.

La propriété du champ est prioritaire. *L'accès normal* peut être modifié par le biais des autorisations.

Autorisation	Description
Voir (R)	Voir le champ, prendre en compte la représentation (Accès normal/protégé en écriture/invisible)
Editer (E)	Voir le champ, prendre en compte la représentation (Accès normal/protégé en écriture/invisible)
<Supprimer> (S)	N'a pas d'effet sur les champs
<Modifier> (E)	N'a pas d'effet sur les champs
<Listes> (L)	N'a pas d'effet sur les champs
<Autorisations> (P)	N'a pas d'effet sur les champs

Modèles de processus

Autorisation	Description
Voir (R)	Voir le modèle, démarrer le processus avec ce modèle
Modifier (W)	Modifier le modèle, créer une nouvelle version du modèle
Supprimer définitivement (D)	
<Modifier> (E)	N'a pas d'effet sur les modèles de processus
<modifier la liste> (L)	N'a pas d'effet sur les modèles de processus
Définir les autorisations (P)	Modifier les autorisations

Processus

Vous pouvez définir les autorisations pour les processus dans le modèle de processus correspondant, en marquant le noeud de processus et en sélectionnant le bouton*Autorisations* dans la section *Général* des réglages de processus.

Autorisation	Description
Voir (R)	Voir le processus (en tant que processus)
Modifier (W)	Modifier le processus après le démarrage
Supprimer définitivement (D)	
Terminer (E)	Le processus n'est pas supprimé et il peut être visualisé dans le client Java ELO dans le dialogue *Aperçu des processus* via le statut *effectué*.

Autorisation	Description
<modifier la liste> (L)	*Pas de répercussions sur les processus.*
Définir les autorisations (P)	Modifier les autorisations

> Les autorisations pour les processus n'ont un impact que lorsque le compte correspondant dispose des droits utilisateurs pour les processus. Vous trouverez d'autres informations au sujet des droits utilisateurs sous Configuration et Administration > Gestion utilisateurs > Droits dans ELO > Droits utilisateur > Droits pour les processus

Les autorisations pour les contenus des teamspaces et workspaces dans ELO sont déterminés via les rôles assignés.

Vous pouvez assigner les autorisations standards suivantes à un rôle pour les contenus dans les teamspaces et workspaces :

Autorisation	Description
Voir (R)	Visualiser une entrée
Modifier les métadonnées (W)	Modifier les métadonnées de l'entrée
Supprimer (D)	Supprimer l’entrée
Modifier (E) (seulement les documents)	Modifier l'entrée sélectionnée, en d'autres termes, modifier la version de travail et charger une nouvelle version
Modifier la liste bearbeiten (L) (seulement les classeurs)	Modifier le contenu du classeur, par exemple, vous pouvez créer des documents dans ce classeur, déplacer ou supprimer des documents à partir de ce classeur.
Définir les autorisations (P)	Modifier les autorisations pour le classeur sélectionné

> Les autorisations n'ont un impact que lorsque le compte correspondant dispose des droits utilisateurs correspondants.

De plus, vous pouvez définir des options d'autorisations pour les entrées qui ont été créées dans un teamspace ou workspace. Vous trouverez de plus amples informations à ce sujet dans la documentation dédiée au Client Java ELO.

Autres autorisations

Les termes *Droits successeurs* et *Droits propriétaire* sont très anciens. Il s'agit d'autorisations.

Droits prédécesseurs

Les droits prédécesseurs sont les autorisations qui sont léguées pour un élément. Les classeurs ont d'autres documents que les sous-entrées. Les documents ont des liens de fichier et des notes en tant que sous-entrées.

Exemple : seul le groupe *Personnel* possède les autorisations pour un document. Le groupe *Tout le monde* possède les autorisations pour les notes qui s'y trouvent. Mais étant donné que seul le groupe *Personnel* a accès au document, *Tout le monde* ne peut pas voir la note dans le document, mai seulement les utilisateurs qui disposent également d'un accès en lecture pour le document.

Lorsqu'un utilisateur ou un groupe a des autorisations sur un document, mais pas d'autorisations pour tout le chemin de dépôt, le document sera affiché après une recherche dans la liste des résultats.

Droits propriétaires

Les droits propriétaire sont un garde-place remplacés par l'utilisateur qui

- a créé un classeur
- a déposé un document
- a apposé un tampon ou une autre remarque sur un document
- a démarré un processus

Tous

Dans une archive ELO, il ne devrait pas y avoir beaucoup d'entrées lisibles par *Tout le monde*.

Pour effectuer une vérification, vous pouvez créer un registre dynamique pour les administrateurs, dans lequel tous les objets lisibles par *tout le monde* sont affichés. Pour ceci, il vous suffit de créer un classeur avec la ligne suivante dans le texte supplémentaire :

```
!+ objekte where objacl='75PYJA' and objstatus=0
```

> **Remarque**
>
> Le groupe *Tout le monde* requiert une autorisation de lecture pour les classeurs personnels, afin que certains services puissent y accéder. Si l'autorisation en lecture est supprimée pour *Tout le monde*, par exemple, les autres utilisateurs ne pourront plus voir la page de profil de cet utilisateur.

Concept pour l'assignations des droits et autorisations.

Introduction

Le concept ci-dessous pour l'assignations des droits et autorisations n'est qu'une recommandation.

Dans ELO, vous avez la possibilité d'associer différents droits utilisateur aux utilisateurs et aux groupes. Les autorisations peuvent également être assignées à différentes entrées et éléments. L'objectif de l'assignation des droits est de conférer à l'utilisateur les droits requis pour qu'il puisse effectuer son travail.

Il est bien sûr possible d'assigner les droits et autorisations au niveau des utilisateurs, mais cela n'est pas toujours très sensé. Au contraire, il vaut mieux organiser les utilisateurs possédant les mêmes droits en groupes, et d'assigner les autorisations et droits sur la base de ces groupes.

Cette documentation a pour sujet la création de groupes pour l'assignation des droits et autorisations. L'intention est de simplifier le concept, de manière à ce qu'il puisse être réalisé sans problèmes dans ELO.

Les droits et autorisations dans l'archive ELO devraient correspondre aux tâches de l'utilisateur dans la société. Les questions suivantes sont primordiales :

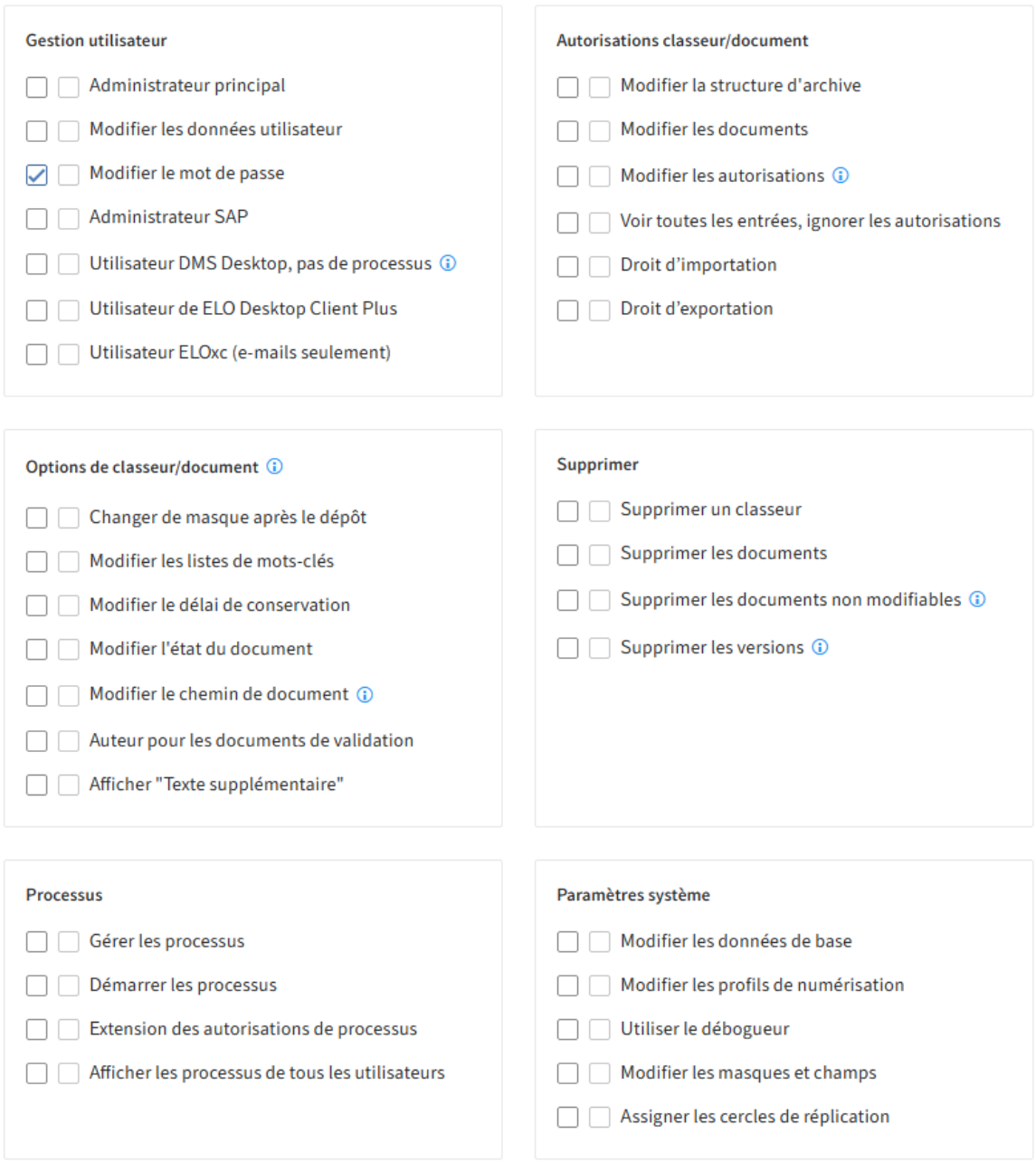
- Quelles sont les tâches de l'utilisateur dans la société ?
- Dans quels services de la société l'utilisateur est-il impliqué ?
- Quelles informations et surtout quels documents sont pertinents pour l'utilisateur afin qu'il puisse effectuer ses tâches ?

Assignation des droits utilisateur

En réponse aux fonctions du collaborateur, l'on peut procéder à l'assignation des droits utilisateur. L'on peut assigner les droits utilisateur en définissant différents groupes d'utilisateur. Dans notre exemple, nous avons défini 5 différents groupes utilisateur.

L'utilisateur ELO View

Les membres de ce groupe ne peuvent que faire afficher les classeurs et documents; le cas échéant, il peut apposer des annotations et notes ou écrire des articles dans le fil d'actualité. Vous n'avez pas le droit d'apporter des modifications aux métadonnées ou de modifier ou encore de supprimer le document en lui-même. Les personnes effectuent des recherches dans l'archive, mais elles n'apportent pas de contenu.



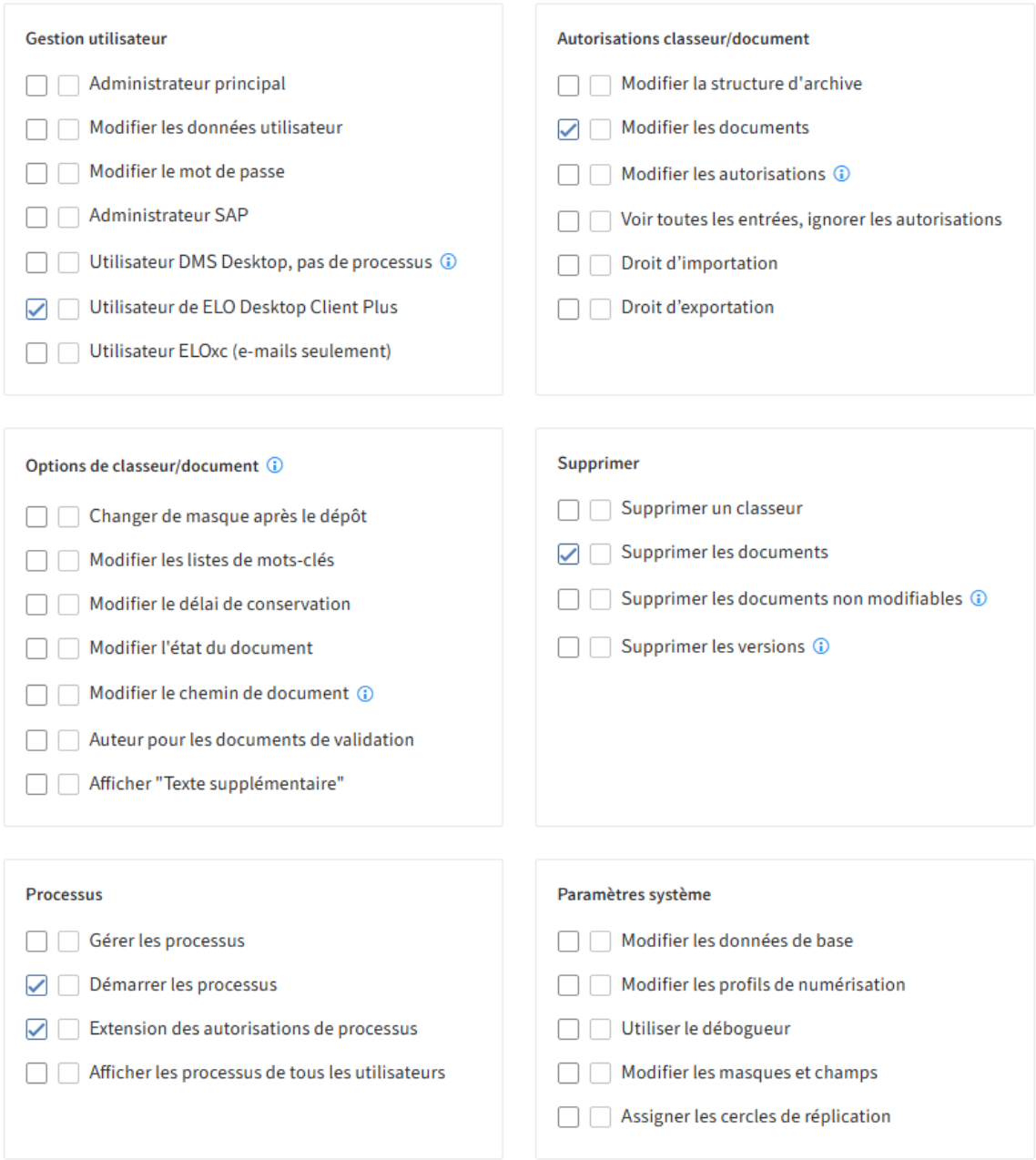
Le groupe de rôles ELO_ViewUsers (droits minimums) peut avoir le droit suivant :

- Modifier le mot de passe

Utilisateur ELO standard

Les membres de ce groupe disposent déjà de droits avancés, qui permettent le traitement de documents et de métadonnées. En fonction des droits octroyés, ces utilisateurs peuvent modifier ou supprimer les documents et les classeurs, modifier, imprimer et exporter les métadonnées, démarrer et modifier les processus.

Ces utilisateurs ont normalement pour tâche de déposer de nouveaux documents dans ELO et/ou de les traiter.



Le groupe de rôles ELO_StandardUsers (droits de base pour le traitement de documents) peut avoir les droits suivants :

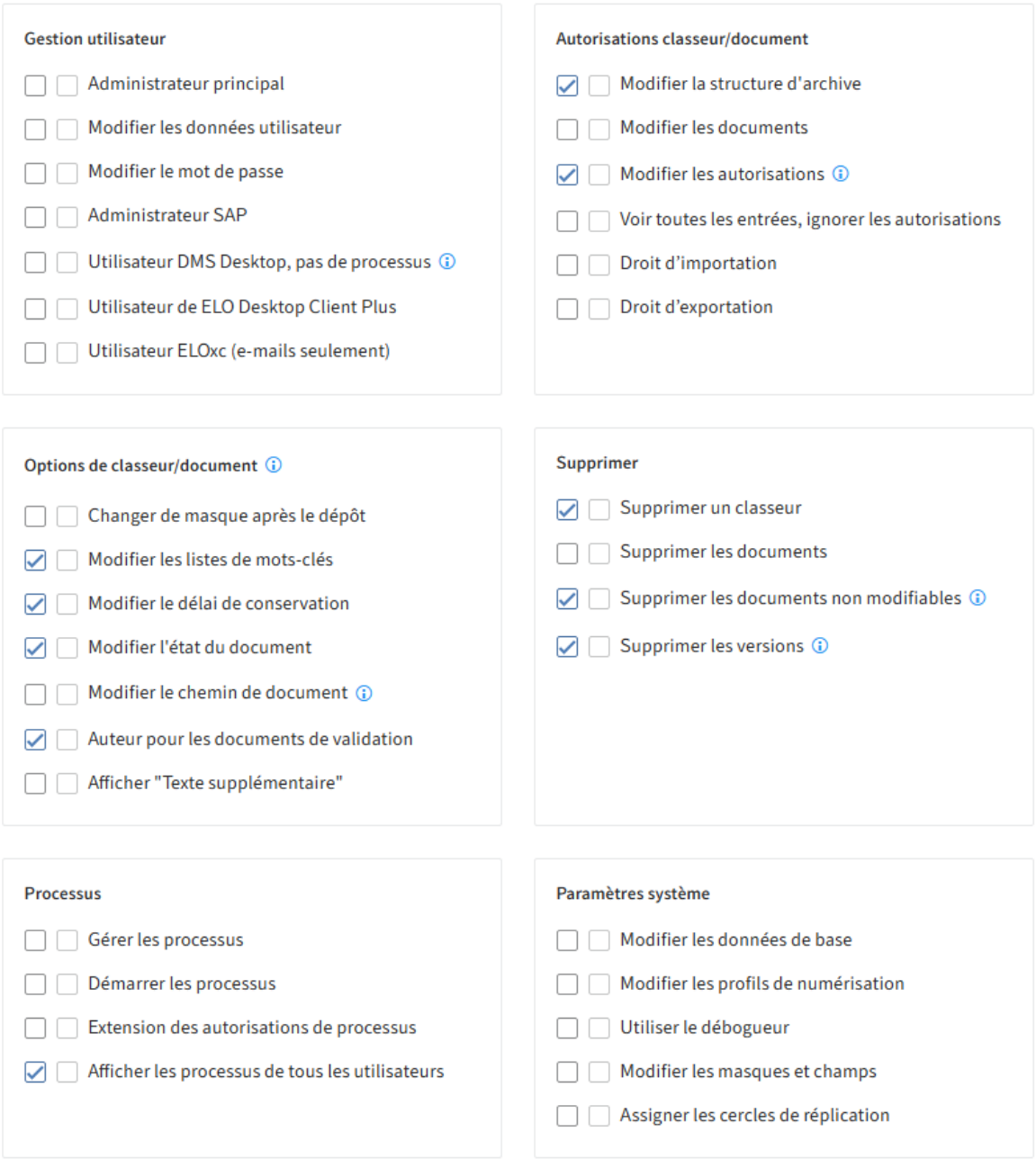
-

Utilisateur ELO Desktop Client Plus
- Traiter les documents
- Supprimer les documents
- Démarrer un processus
- Extension des autorisations de processus

ELO Power-User

Les membres de ce groupe ont plus de droits concernant les tâches dans ELO. Normalement, ils sont chargés de traiter la structure de classeurs dans ELO ainsi que le concept des autorisations. Ils sont chargés de réaliser la structure d'archive avec des classeurs statiques ou dynamiques, ou avec des classeurs standards qui peuvent être utilisés par d'autres utilisateurs.

Ils peuvent modifier les documents et les options de documents, ainsi que les dates d'expiration et les statuts de document. Ils peuvent supprimer les documents qui ne sont pas supprimables et les différentes versions. Ils peuvent également contrôler l'état des processus auxquels ils ne participent pas activement.



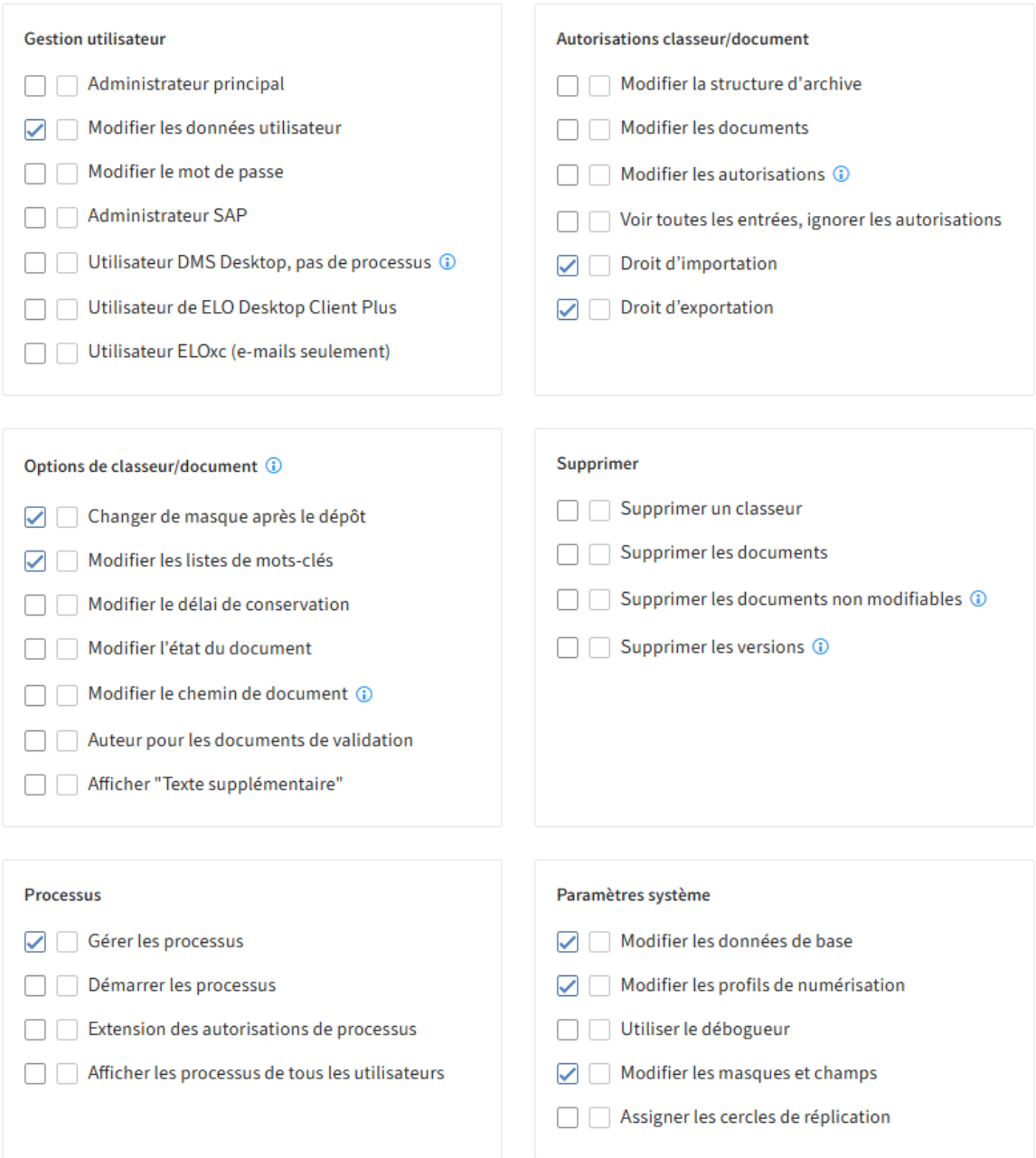
Le groupe des rôles ELO_PowerUsers (droits étendus et traitement de la structure de classeurs) peut avoir les droits suivants :

- Modifier les classeurs
- Supprimer un classeur
- Modifier les autorisations
- Modifier la liste des mots-clés
- Modifier le délai de conservation
- Auteur pour les documents de validation
- Supprimer les versions
- Afficher les processus de tous les utilisateurs (contrôler)
- Supprimer les documents non modifiables
- Modifier l'état du document

L'administrateur ELO spécialisé

Les membres de ce groupe peuvent gérer les réglages dans l'archive pour les administrateurs qu'ils administrent eux-mêmes et gérer leur remplacements. La plupart du temps, ils sont mis en place en tant qu'administrateur de leur propre service. Ils connaissent les processus internes et créent les modèles de processus requis. Ils savent quelles données sont importantes lors du dépôt et définissent les masques et listes de mots-clés requis. Ils peuvent créer des tampons et modifier les couleurs d'écriture.

L'administrateur ELO spécialisé est moins responsable que d'autres du traitement et du travail avec les documents. Il est chargé de la structure de l'archive, des processus, et se charge des tâches de surveillance.



Le groupe de rôles ELO_FachAdministratoren (réglages dans l'archive) peut avoir les droits suivants :

-

Autorisation d'importation
- Droit d’exportation
- Modifier les masques et champs
- Modifier la liste des mots-clés
- Changer de masque après le dépôt
- Modifier les données de base
- Gérer les processus
- Modifier les données utilisateur (seuls les utilisateurs qu'il administre lui-même)
- Modifier les profils de numérisation

L'administrateur ELO

Les membres de ce groupe peuvent gérer les réglages de la configuration, des profils de numérisation, des remplacements et des données utilisateurs pour d'autres utilisateurs. Ils peuvent gérer des unités d'organisation, assigner des cercles de réplication, retirer les verrouillages et gérer les fichiers document dans le système de fichiers, les déplacer, les enregistrer dans une sauvegarde ou encore les supprimer définitivement.

Les administrateurs ELO n'effectuent pas de tâches liées directement aux classeurs ou documents de l'archive; ils sont responsables de l'administration de l'archive.

Gestion utilisateur

- [x] Administrateur principal
- [x] Modifier les données utilisateur
- [ ] Modifier le mot de passe
- [x] Administrateur SAP
- [ ] Utilisateur DMS Desktop, pas de processus
- [ ] Utilisateur de ELO Desktop Client Plus
- [ ] Utilisateur ELOxc (e-mails seulement)

Autorisations classeur/document

- [ ] Modifier la structure d'archive
- [ ] Modifier les documents
- [ ] Modifier les autorisations
- [ ] Voir toutes les entrées, ignorer les autorisations
- [ ] Droit d'importation
- [ ] Droit d'exportation

Options de classeur/document

- [ ] Changer de masque après le dépôt
- [ ] Modifier les listes de mots-clés
- [ ] Modifier le délai de conservation
- [ ] Modifier l'état du document
- [x] Modifier le chemin de document
- [ ] Auteur pour les documents de validation
- [x] Afficher "Texte supplémentaire"

Supprimer

- [ ] Supprimer un classeur
- [ ] Supprimer les documents
- [ ] Supprimer les documents non modifiables
- [ ] Supprimer les versions

Processus

- [ ] Gérer les processus
- [ ] Démarrer les processus
- [ ] Extension des autorisations de processus
- [ ] Afficher les processus de tous les utilisateurs

Paramètres système

- [ ] Modifier les données de base
- [x] Modifier les profils de numérisation
- [x] Utiliser le débogueur
- [ ] Modifier les masques et champs
- [x] Assigner les cercles de réplication

Concept de groupes et d'autorisations

Il est sensé de regrouper les fonctions et les autorisations dans différents groupes.

Pour associer différentes autorisations aux différentes sections d'archive, nous vous recommandons de créer des groupes spécifiques. L'exemple suivant vous explique comment l'on pourrait conceptionner l'association de droits par le biais de groupes et de groupes OU.

Association d'autorisations à des groupes

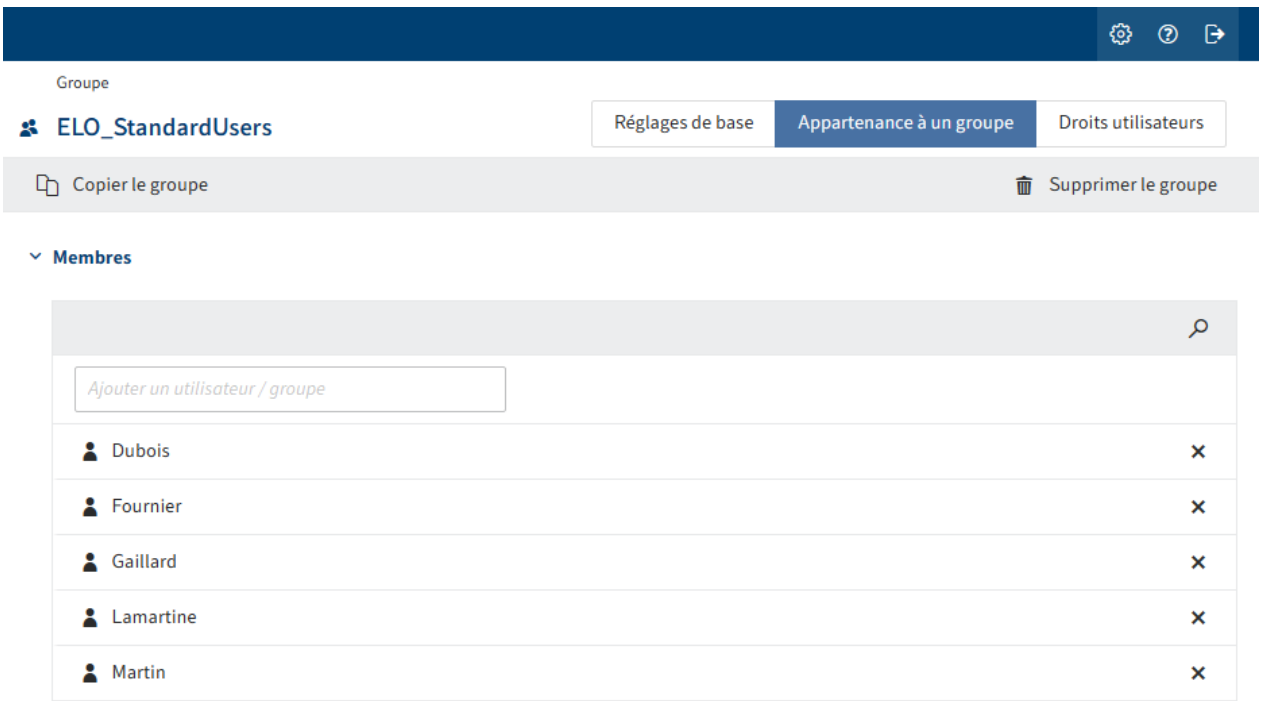
La société se compose des services Personnel, Production et Logistique. Différentes autorisations d'accès ont été créées dans l'archive pour les différents services.

L'association aux différents services gère également les autorisations aux documents de l'archive. Dans notre exemple, les membres du service RH peuvent accéder à tous les documents de la section Personnel, les membres du service production, à la section Production, et les membres du service de logistique, à la section Logistique. En conséquent, les groupes sont créés conformément aux différents services de la société.

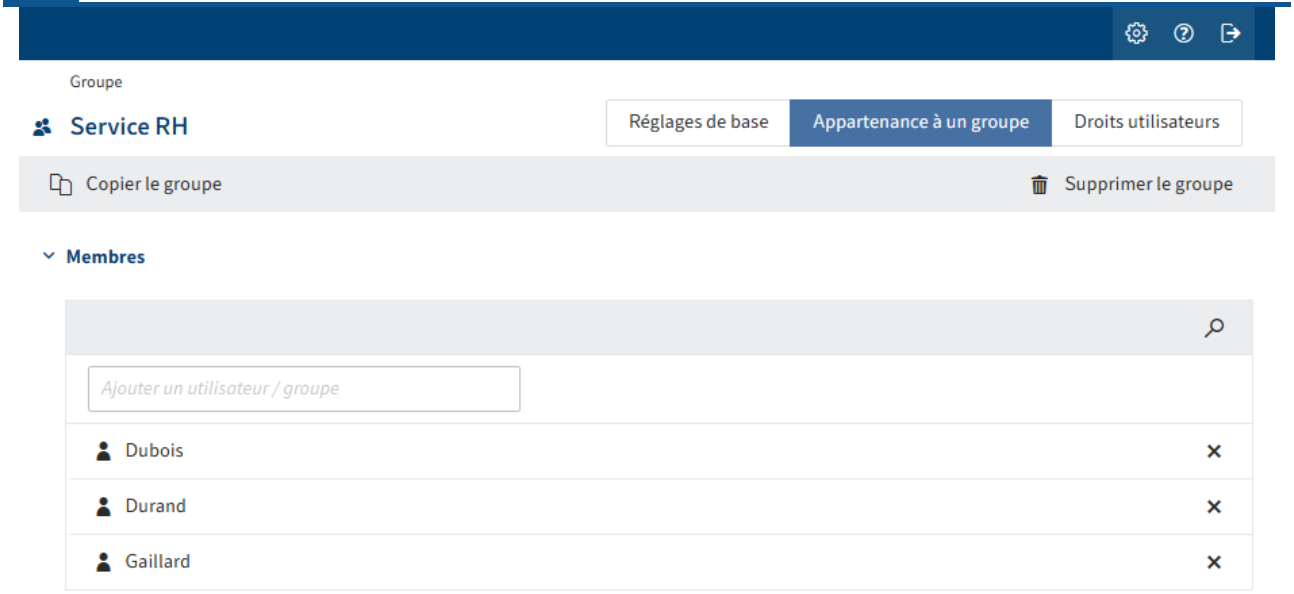
Les groupes par le biais desquels les droits utilisateurs sont associés, sont nommés groupes de rôles. Ceux-ci sont combinés avec les groupes d'appartenance aux services.

Les droits utilisateurs devraient toujours être liés à un groupe et non pas à un utilisateur. L'association des droits peut se faire de manière transparente.

Nous avons les membres suivants dans le groupe de rôles de notre exemple.

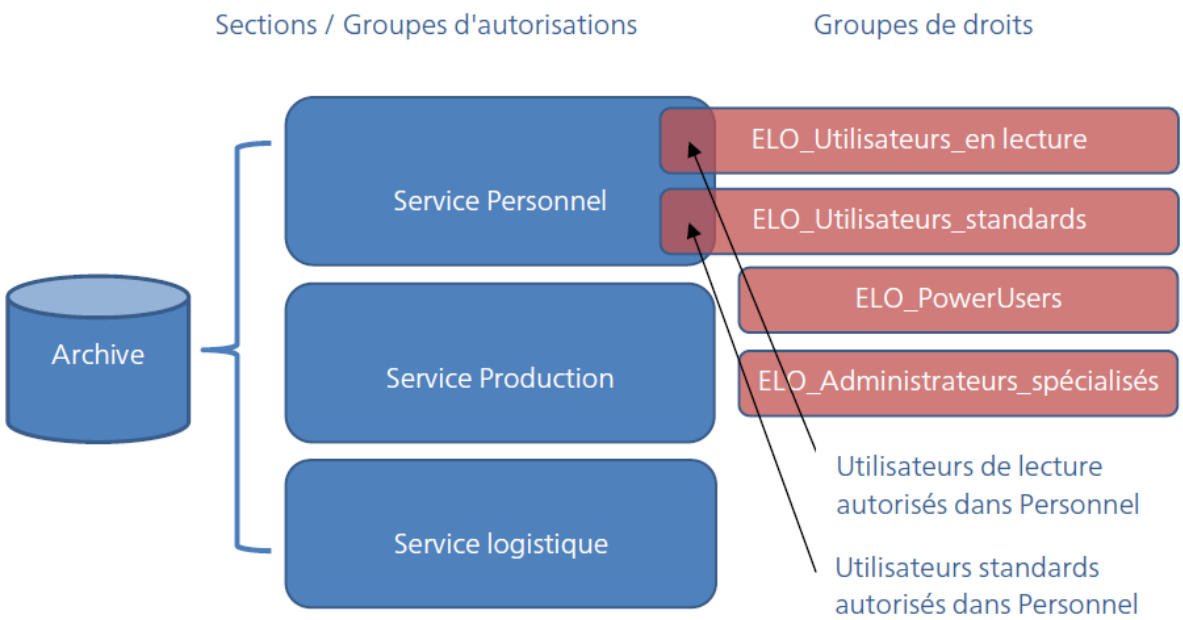


Nous avons les membres suivants travaillent dans le groupe de rôles *Service RH*. Seuls ces collaborateurs ont accès aux documents du service *Personnel*.



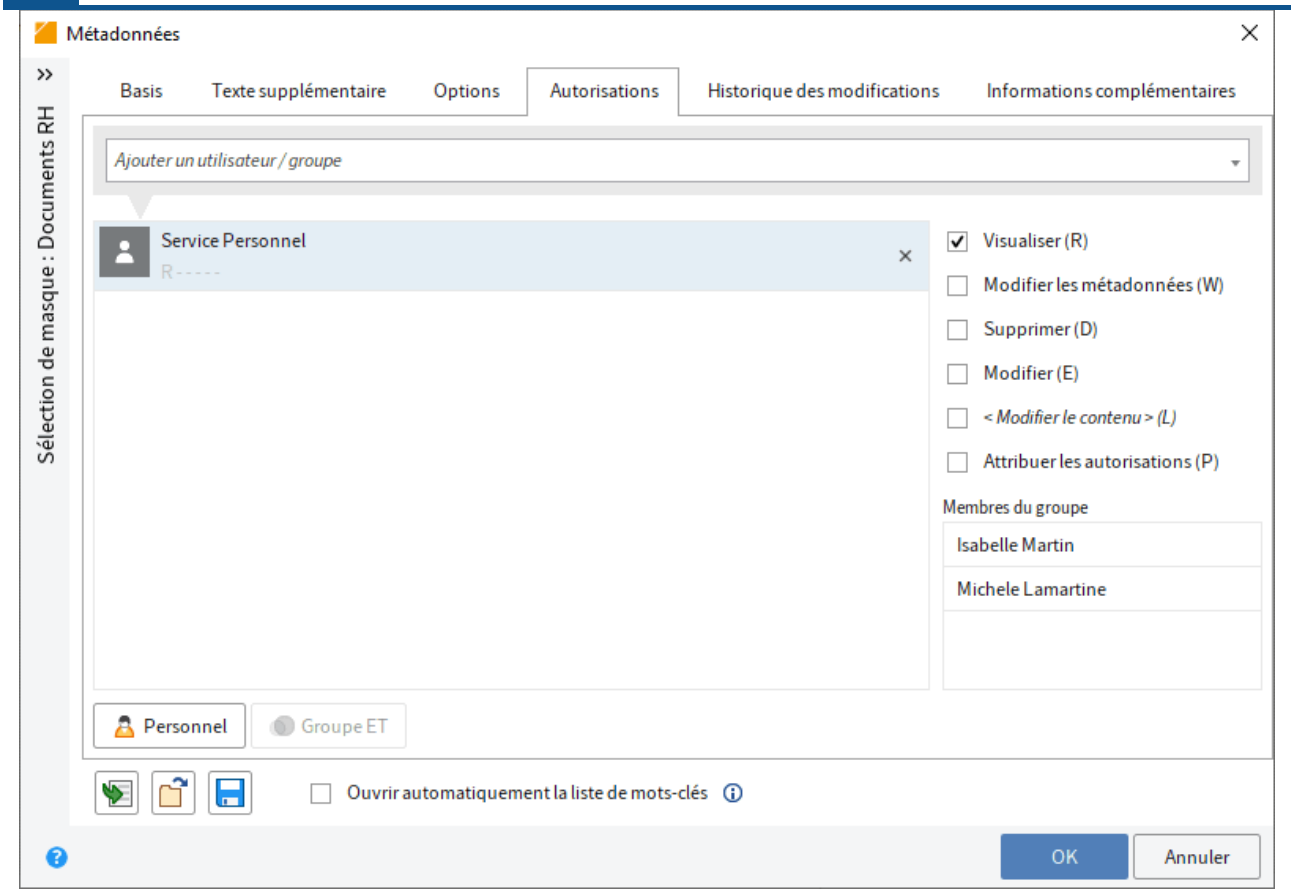
Utilisation de groupes ET

L'illustration suivante reflète l'assignation des autorisations dans le service des ressources humaines.

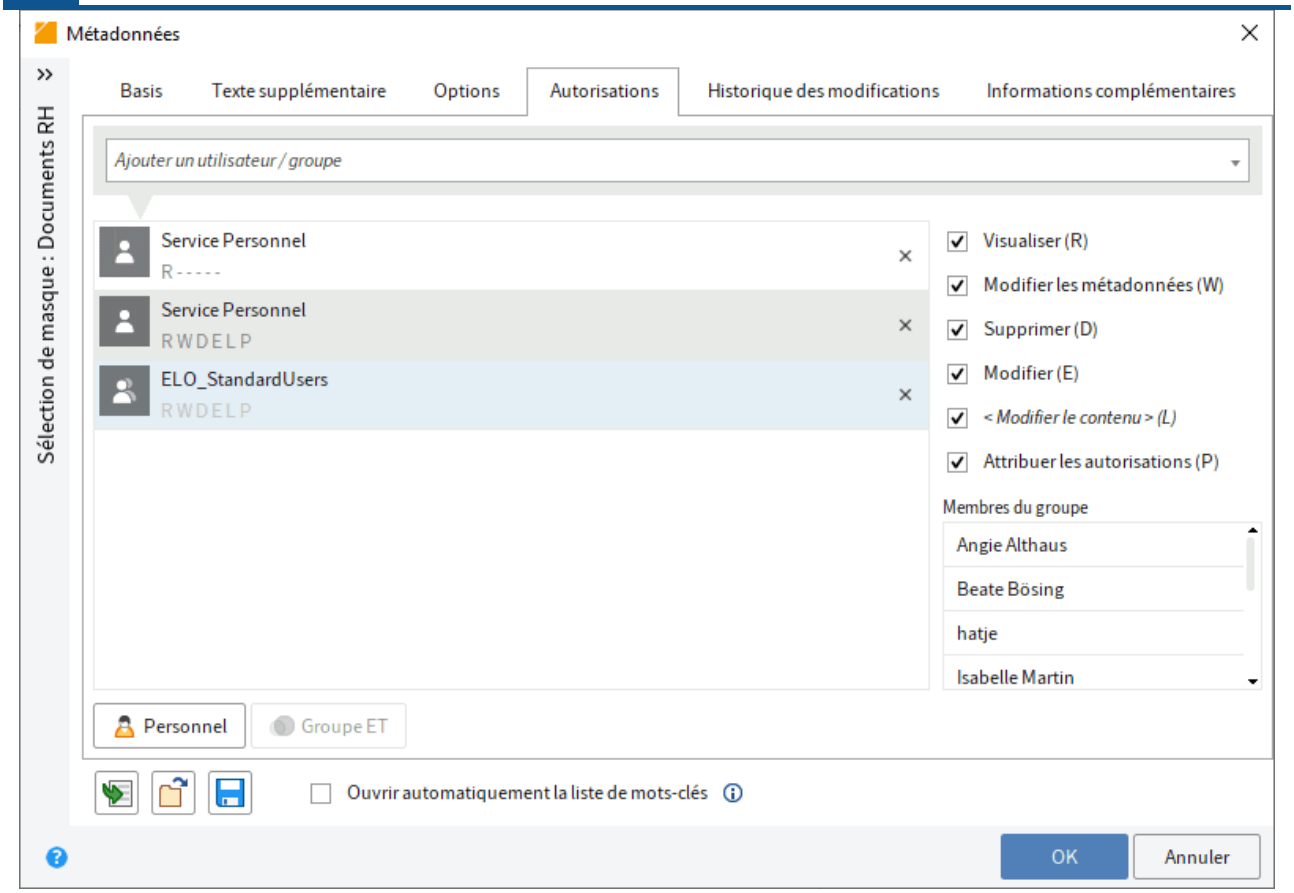


Maintenant, nous pouvons déterminer les autorisations sur les documents et classeurs dans le service *Service RH* à l'aide d'un groupe ET : les autorisations valent pour les membres qui sont aussi bien dans le groupe *Personnel* que dans le groupe *ELO_Utilisateurs_standards*.

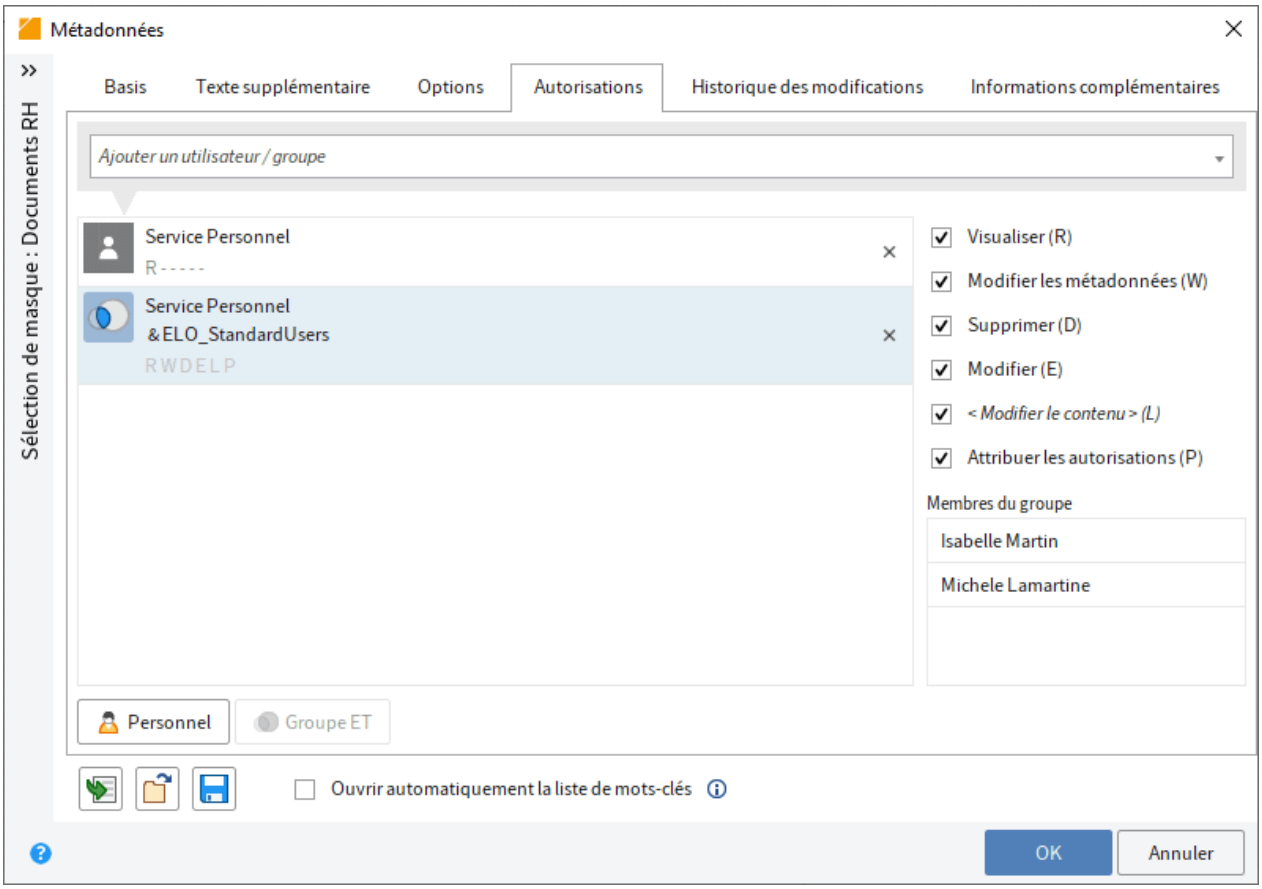
Par exemple, vous pouvez déterminer que tous les membres du *service RH* ont le droit de lire le document correspondant.



Pour être sur que seuls les *utilisateurs ELO standards* ont un accès intégral à ce document dans le groupe *Service RH*, nous créons un groupe ET. Un groupe ET contient les dénominateurs communs des groupes sélectionnés.

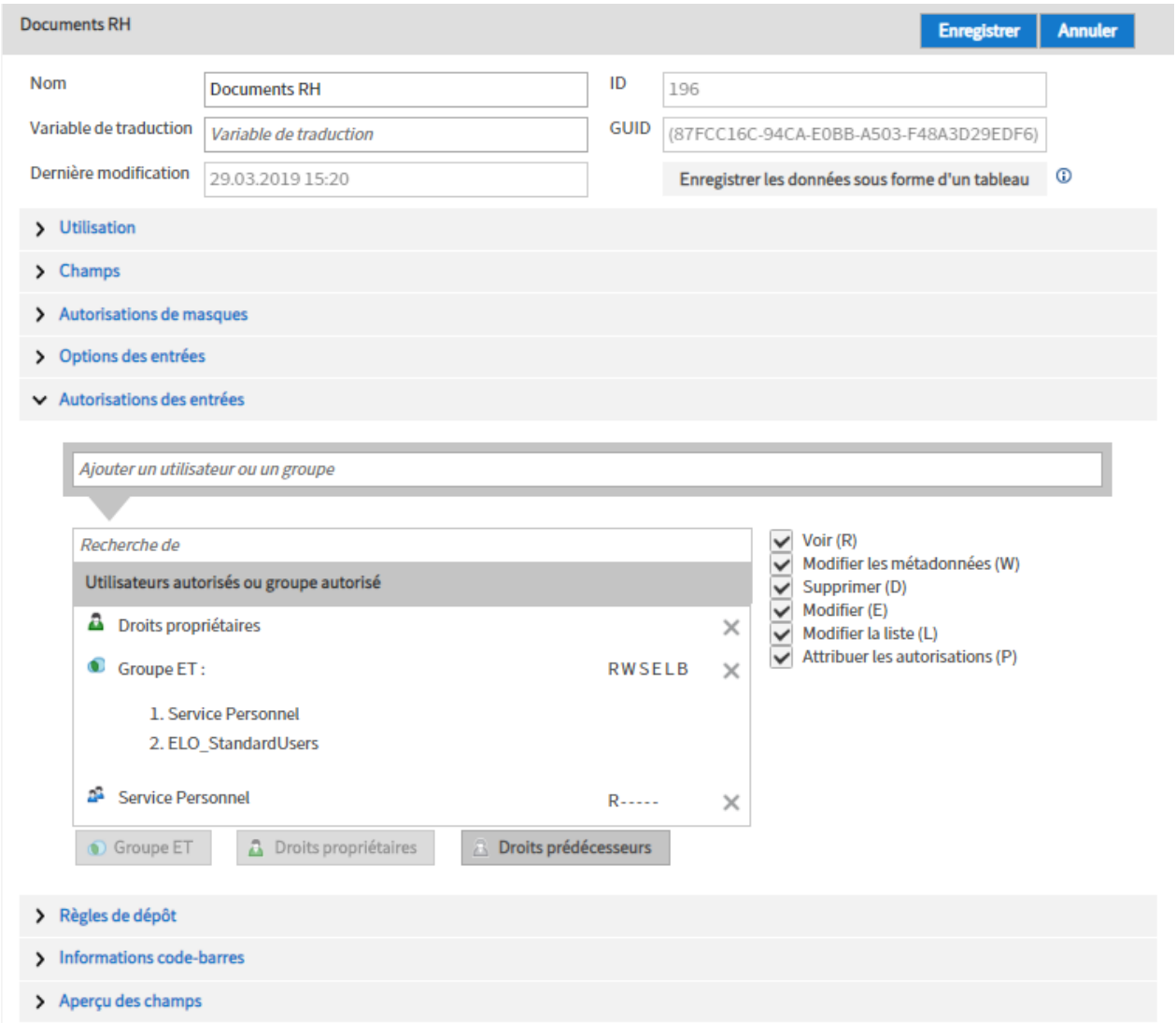


Dans notre exemple, les membres du groupe ET ont un accès intégral à ce document. ELO affiche de quels utilisateurs il s'agit.



Assignation des autorisations par le biais de masques

Pour être sûr que les documents RH ne puissent être traités que par les utilisateurs autorisés, nous vous recommandons de définir ces autorisations par le biais du masque, et non pas pour les différentes entrées distinctes dans l'archive.



LDAP

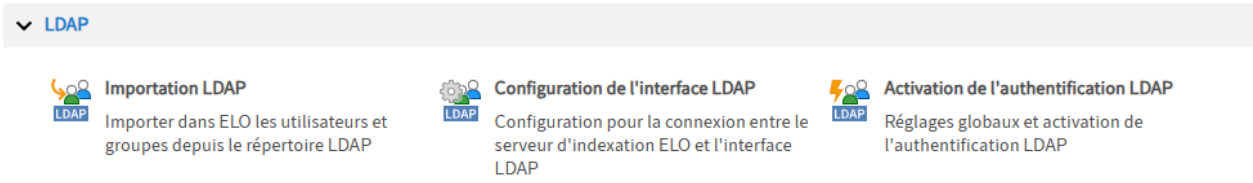
Introduction

A l'aide de Lightweight Directory Access Protocol (LDAP), il est possible de copier les utilisateurs et groupes depuis un Active Directory (AD) dans le système ELO. Cela se fait via l'importation LDAP.

Afin que l'importation LDAP puisse être effectuée, la connexion entre LDAP et l'interface LDAP ELO peut être établie et configurée.

De plus, l'authentification LDAP doit être activée, afin que les utilisateurs puissent se connecter à ELO avec les données enregistrées dans Active Directory.

Vous trouverez les points de menu dans la console d'administration ELO sous *LDAP*.



Dans le répertoire LDAP, la gestion utilisateurs se fait dans une arborescence. Un nom univalent est utilisé en tant que clé univalente au sein du répertoire LDAP, le `distinguished name` (DN). Un exemple pour un DN est `cn=John Doe,ou=people,dc=comy,dc=org`. Le nom univalent se compose de trois parties : le `common name` (CN), le `organizational unit` (OU) et le `domain component` (DC). Avec la combinaison OU/DC; il est possible de référencer différentes branches dans la structure d'arborescence LDAP. DC sert à adresser le niveau supérieur, sous le noeud racine du répertoire LDAP. En règle générale, c'est le domaine internet de la société qui est représenté. Les données de schéma se trouvent également directement sous le noeud racine. Les différents attributs sont indiqués dans le schéma LDAP et les valeurs correspondants à ces propriétés sont fournies dans l'entrée LDAP.

> **Remarque**
>
> Dans Active Directory (AD), n'utilisez pas de ; dans les noms de groupe et noms utilisateur.

Configuration de l'interface LDAP

Dans la console d'administration, le point de menu *Configuration de l'interface LDAP* vous permet de modifier le fichier de configuration *ldap.json* concernant les données de connexion, la sélection des utilisateurs et l'assignation des attributs. Le fichier *ldap.json* es enregistré dans l'archive sous le chemin suivant :

Administration // IndexServer Scripting Base // _ALL // ldap.json

Information

Les modifications de champ sont possibles dans les cas suivants :

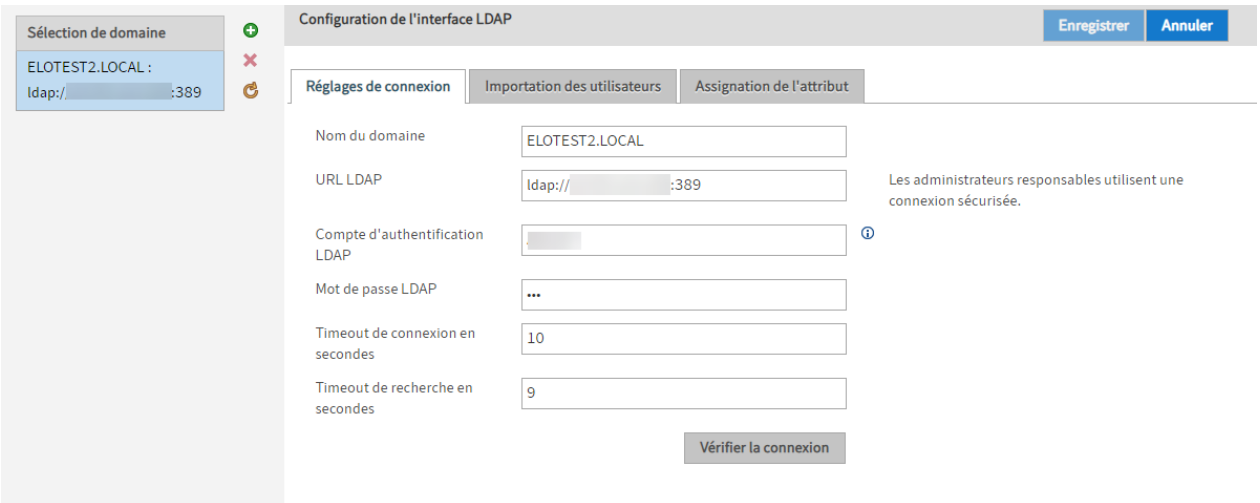
- Si vous souhaitez effectuer une configuration spécifique pour un serveur d'indexation ELO, copiez le fichier dans le répertoire du serveur d'indexation ELO correspondant et ajustez le fichier à cet emplacement.
- Si vous souhaitez effectuer différentes configurations pour différents serveurs d'indexation ELO, il vous faut un propre fichier pour chaque serveur d'indexation ELO.

La configuration se réfère à une seule archive. Si la configuration est effectuée par le biais de la console d'administration ELO, le serveur d'indexation ELO de l'archive doit être redémarré. S'il existe plusieurs serveurs d'indexation ELO, ils doivent tous être redémarrés.

Remarque

Le compte ELO Service (ou le compte de service utilisé) ne devrait pas être authentifié via LDAP. Ainsi, les applications ELO basés serveur sont indépendants de la configuration LDAP. Sinon, la désactivation de la connexion LDAP peut avoir pour effet que les applications ELO ne démarrent plus. Une activation de l'interface LDAP ne sera alors plus possible via la console d'administration.

Les comptes administratifs ne devraient pas être authentifiés via LDAP.



Vous pouvez effectuer des réglages pour plusieurs domaines.

Dans la section *Sélection de domaine*, vous voyez tous les domaines existants.

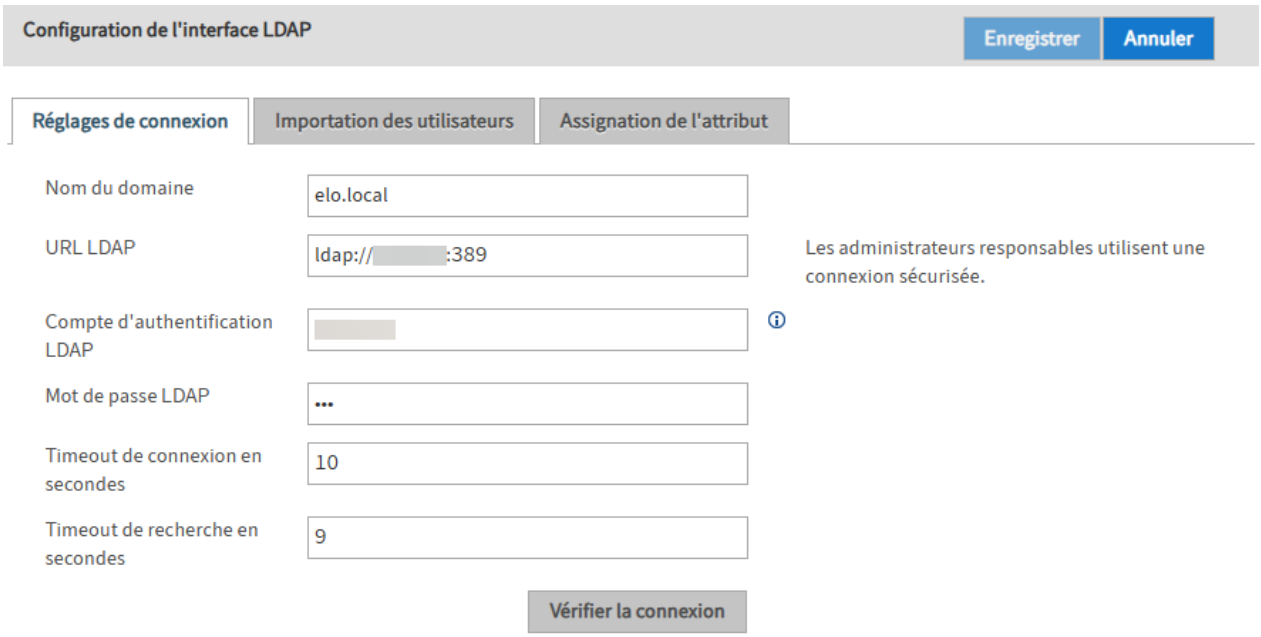
Ajouter (symbole plus vert) : ajouter des réglages pour un domaine.

Supprimer (symbole x rouge) : supprimer les réglages pour un domaine.

Récupérer à nouveau les données du serveur (symbole avec deux flèches rondes jaunes) : actualiser la section *Sélection du domaine*

> **Information**
>
> En cas de problèmes de connexion, le fichier log du serveur d'indexation ELO peut passer à *debug*. Cela permet de simplifier la recherche d'erreurs.

Réglages de connexion



Nom du domaine : entrez le nom DNS ou l'adresse IP du domaine dans cette option. Le réglage est utilisé lorsque `userPrincipalName` est formé à partir de `sAMAccountName`.

URL LDAP : les entrées dans le champ *URL LDAP* permettent de déterminer la connexion vers le serveur LDAP par le biais de TCP.

Compte d'authentification LDAP : Pour SSO, un compte technique est requis, permettant de rechercher le compte utilisateur transmis par le mécanisme SSO - en règle générale, il s'agit de `sAMAccountName` - dans LDAP. Veuillez indiquer un `userPrincipalName`.

> **Remarque**
>
> Le compte doit avoir des droits suffisants pour lire les attributs utilisateurs et les appartenances de groupe.

> **Remarque**

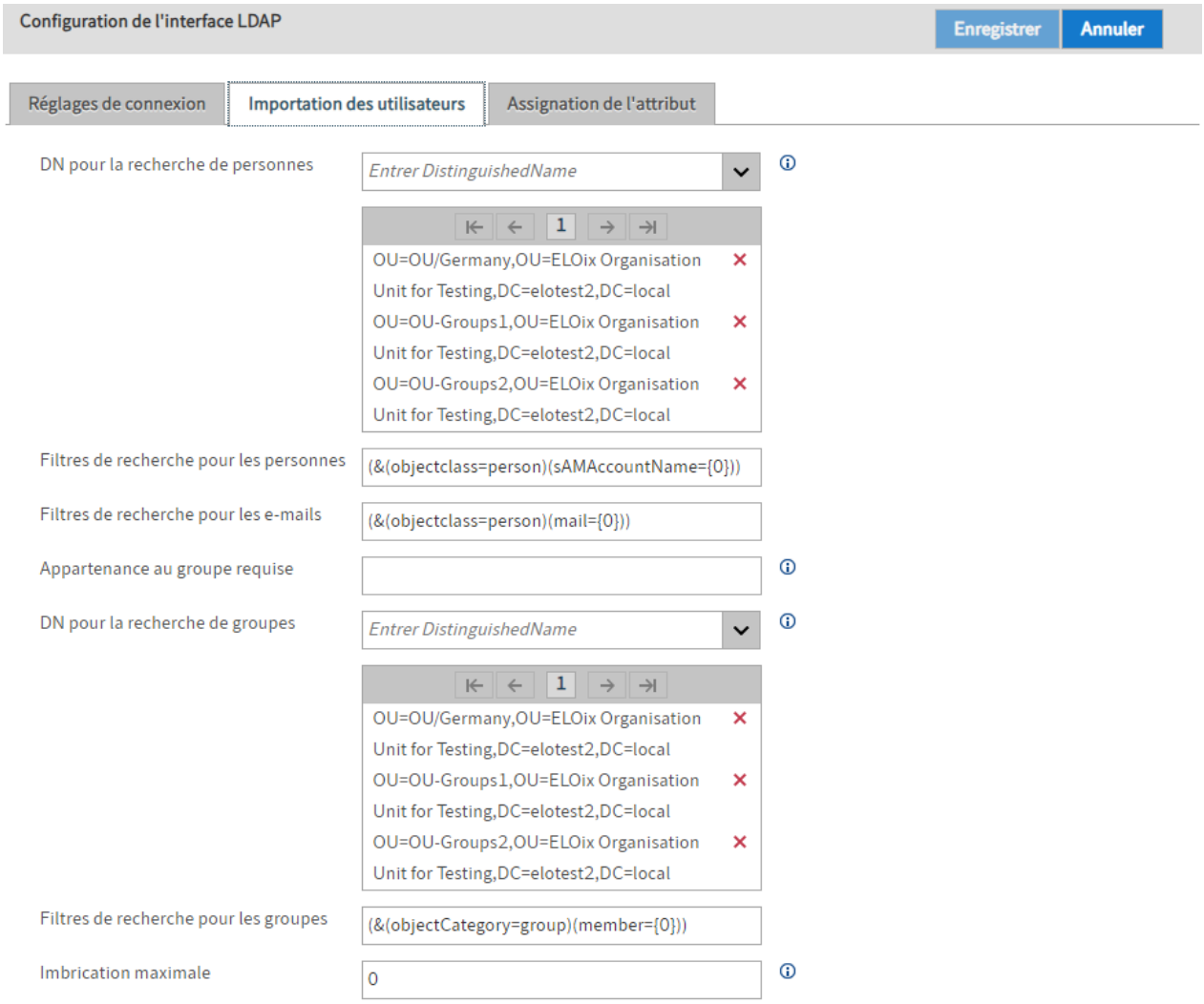
> Si vous utilisez Kerberos : déconnectez le compte Kerberos et le compte LDAP. Le compte Kerberos ne doit pas exister dans ELO.

Mot de passe LDAP : vous pouvez entrer le mot de passe crypté du compte d'authentification LDAP dans le champ *Mot de passe LDAP*. Le serveur d'indexation ELO l'enregistre de manière cryptée lors d'un redémarrage.

Timeout de connexion en secondes : l'interface LDAP interrompt une tentative de connexion au serveur LDAP après ce nombre de secondes. Ensuite, c'est le prochain serveur dans la liste qui est testé.

Timeout de recherche en secondes : lors d'une recherche d'utilisateurs ou de groupes, cette valeur de timeout est transmise au serveur LDAP.

Importation des utilisateurs



DN pour la recherche de personnes : ce champ vous permet d'indiquer dans quelles branches du répertoire LDAP vous souhaitez effectuer une recherche d'utilisateurs.

> **Remarque**

La liste ne doit pas être vide.

N'indiquez pas trop de branches. Plus vous indiquez de branches, moins la recherche sera précise.

Filtres de recherche pour les personnes : la recherche des utilisateurs peut être limitée avec ce filtre.

Filtres de recherche pour les e-mails : lors de la première authentification avec l'adresse e-mail, l'utilisateur est recherché dans le répertoire LDAP par le biais de cette filtre.

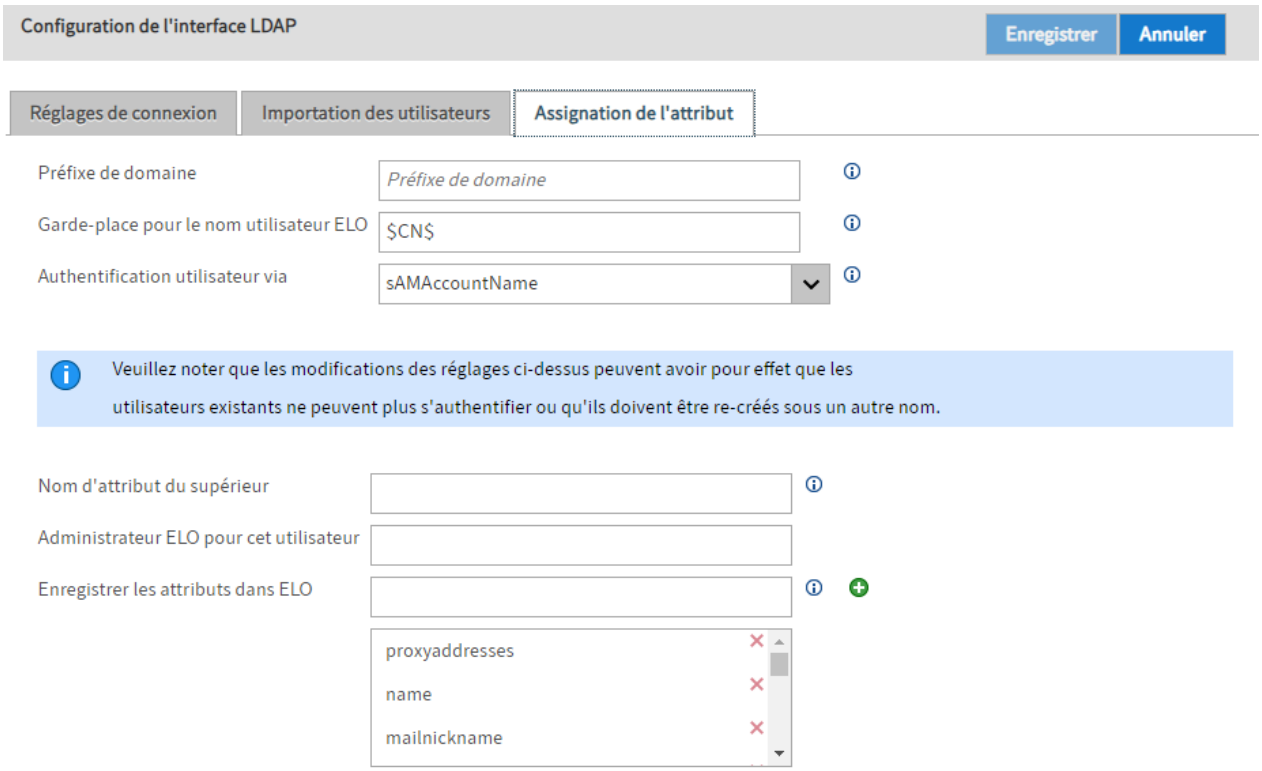
Appartenance à un groupe : ce champ permet de limiter l'authentification aux utilisateurs qui sont membres d'un groupe précis dans le répertoire LDAP. L'indication doit être faite en tant que Common Name.

DN pour recherche de groupe : dans ce champ, nous déterminons dans quelles branches du répertoire LDAP doivent se trouver les groupes qui entrent en compte pour l'ajustement des groupes. Si la liste est vide, tous les groupes de l'utilisateurs seront pris en compte.

Recherche de filtre pour les groupes : la recherche des groupes d'un utilisateur peut être limitée avec ce filtre.

Imbrication maximale : ce champ permet d'indiquer la profondeur du rapport groupe dans le groupe. Cela se réfère lors du rassemblement de groupes utilisateurs pour la synchronisation du groupe.

Assignation d'un attribut



Préfixe de domaine : le préfixe de domaine est requis lorsque plusieurs domaines doivent être configurés et que `sAMAccountName` est un utilisateur Windows (voir le réglage attributeForUserPropOS).

Le préfixe de domaine doit terminer par un caractère de séparation. Cela permet de séparer le préfixe du nom utilisateur. Nous vous recommandons d'utiliser un backslash.

> **Information**
>
> Si vous souhaitez utiliser SSO, le préfixe de domaine doit concorder avec le nom de domaine court (NetBIOS).

Le préfixe de domaine concordant avec SSO se trouve sur l'ordinateur client dans la variable d'environnement `USERDOMAIN`. Remarque : pour SSO avec préfixe de domaine, l'option `"ntlm.domainUserFormat"` doit être activée dans le fichier *config.xml* du serveur d'indexation ELO (voir). Si *sAMAccountName* est sélectionné dans le champ `Connexion via` et qu'un préfixe de domaine domainPrefix est sélectionné, l'utilisateur Windows obtient le nom du compte avec un préfixe de domaine.

Exemple :

- `sAMAccountName` = claudinedupont
- Préfixe de domaine = ELO\
- Utilisateur Windows = ELO\claudinedupont

Garde-place pour les noms utilisateur ELO: le nom utilisateur ELO peut se composer depuis différents attributs LDAP de l'utilisateur. Pour ceci, vous pouvez indiquer une expression de format avec des gardes-places. Les gardes-places sont encadrés entre des caractères $ et correspondent aux noms attributs LDAP.

Authentification utilisateur par le biais de : le menu déroulant *Authentification utilisateur par le biais de* vous permet de sélectionner si vous souhaitez utiliser *sAMAccountName*, `userPrincipalName` ou `UID` pour la propriété Utilisateur Windows.

> **Remarque**
>
> Le réglage sélectionné dans le champ *Authentification utilisateur par le biais de* doit concorder avec les réglages dans le champ *Filtre de recherche pour les utilisateurs* (onglet *Assignation des utilisateurs*). Veuillez respecter la casse.
>
> L'utilisation des trémas devrait être la même dans Active Directory et pour les noms utilisateur.
>
> La console d'administration ELO vérifie les 4 attributs suivants sur la page LDAP. La console d'administration ELO utilise le premier attribut pour le nom.
>
> ```
> LdapServerFactory.CONST.USERINFO.DISPLAY_NAME,
> LdapServerFactory.CONST.USERINFO.CN,
> LdapServerFactory.CONST.USERINFO.SAM_ACCOUNT_NAME
> LdapServerFactory.CONST.USERINFO.DISTINGUISHED_NAME
> ```

Information

Une configuration individuelle est nécessaire pour certains environnements. Le champ permet une saisie libre de valeurs.

Nom d'attribut du supérieur : ce champ vous permet de déterminer à partir de quel attribut est défini le supérieur de l'utilisateur ELO. En règle générale, c'est l'attribut `$manager$` qui est utilisé.

Remarque

Le supérieur doit déjà exister dans ELO.

Administrateur ELO pour cet utilisateur : pour les utilisateurs créés par l'interface LDAP, le champ *Administrateur ELO pour cet utilisateur* permet de déterminer quel utilisateur ELO doit être assigné en tant qu'administrateur. L'indication peut être faite sous forme d'ID, de GUID ou de nom utilisateur ELO.

Enregistrer les attributs dans ELO : ce champ vous permet de déterminer quels attributs de LDAP doivent être transférés dans ELO.

Pour ajouter un attribut, veuillez entrer le nom de l'attribut dans le champ. Cliquez ensuite sur *Ajouter* (symbole + vert).

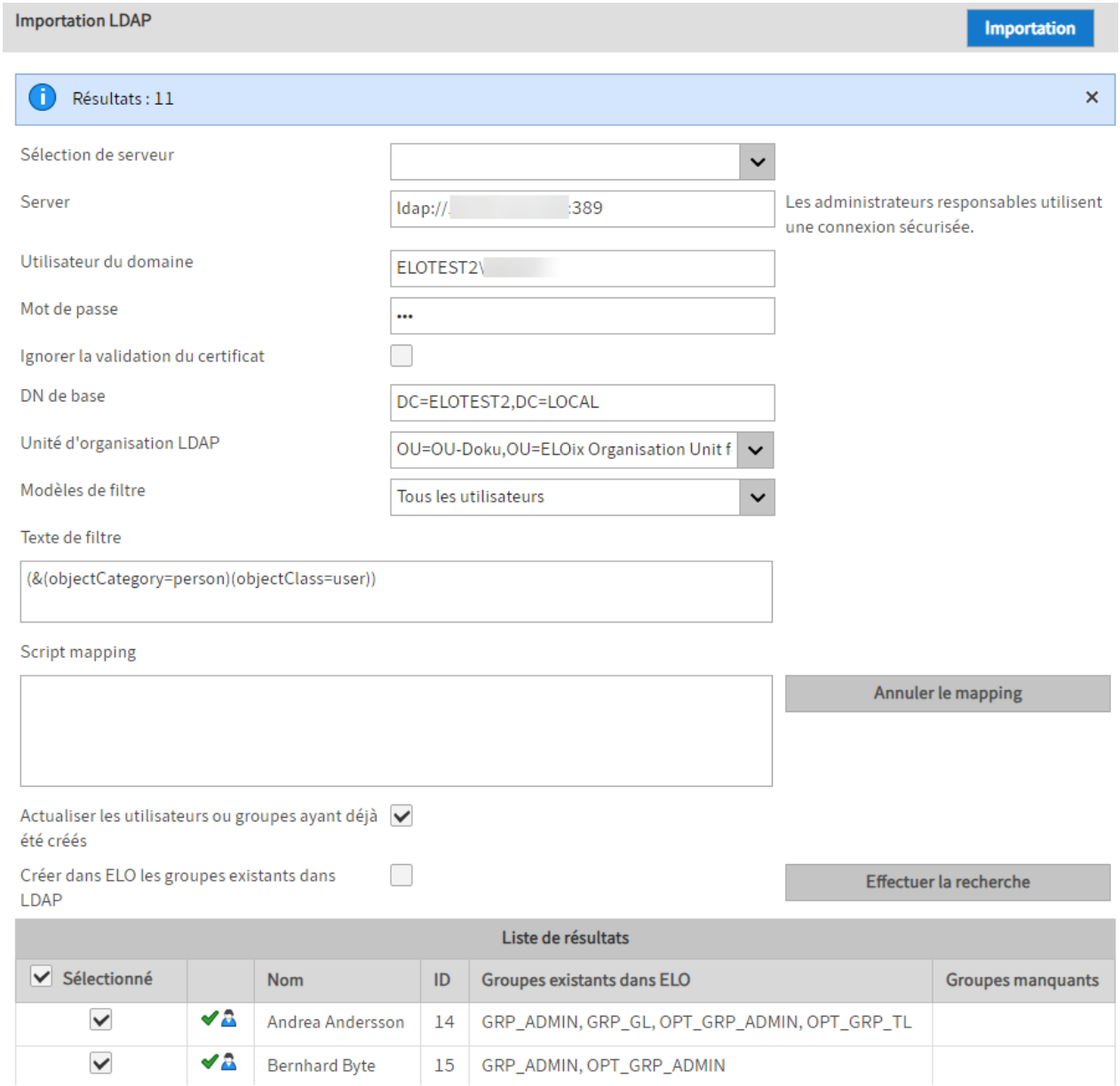
Pour supprimer un attribut, cliquez sur le symbole X correspondant dans la liste des attributs.

Information

Les attributs obligatoires ne peuvent pas être supprimés de la section des tâches. Dans ce cas, le symbole X est grisé.

Importation LDAP

Avec l'importation LDAP, vous pouvez copier les utilisateurs et groupes dans le système ELO depuis un Active Directory (AD).



- Sélection du serveur : La console d'administration ELO essaie automatiquement de trouver des serveurs LDAP. Lorsque ce champ de sélection est vide, aucun serveur n'est trouvé dans le domaine. Par exemple, cela peut être le cas pour une connexion VPN.
- Serveur: ici, est entré le serveur de connexion LDAP. Il est également possible d'entrer l'adresse IP, le port ou le protocole ici.

  ```
  BNF: Serveur ::=[ldap|ldaps]://[nom de serveur|adresse IP]:port
  ```

> **Remarque**
>
> Utilisez une connexion sécurisée, dans ce cas, LDAP via SSL (LDAPS).

-

Utilisateur de domaine et mot de passe : les données utilisateur se composent du nom et du mot de passe.

- Ignorer la validation du certificat : le cas échéant, il est possible d'ignorer la validation du certificat.
- DN de base et unité d'organisation LDAP : ces entrées permettent de sélectionner la branche correcte dans le répertoire LDAP.
- Modèles et texte de filtres : certaines expressions de filtre LDAP sont indiquées dans la liste de sélection et se trouvent dans le texte de filtre pour un traitement libre.
- Script de mappage : permet un traitement supplémentaire des données sous forme d'un code JavaScript.

  Vous trouverez de plus amples informations à ce sujet dans le prochain paragraphe *Le script de mappage*.
- Réinitialiser le mappage : supprime le texte dans le champ de script de mappage.
- Actualiser les utilisateurs ou groupes ayant déjà été créés : si le nom d'une entrée existant déjà peut être résolu, cette entrée ne peut être traitée que si la case est cochée.

  > **Remarque**
  >
  > Les groupes LDAP sont seulement extraits et appliqués lors de l'authentification des utilisateurs.

- Créer les groupes existants dans LDAP dans ELO : crée également les groupes qui n'existent pas encore dans ELO.
- Exécuter la recherche : exécute la recherche et affiche les résultats.
- Liste des résultats : affiche la liste des entrées à importer. Toutes les entrées valides sont sélectionnées. Si des données invalides ont été reconnues lors de la vérification, celles-ci ne seront pas sélectionnées et la remarque correspondante est affichée sous forme d'une infobulle.

Le script de mappage

Il existe un mappage prédéfini d'attributs LDAP standards sur les attributs ELO. Il est possible d'ajouter un code JavaScript dans le champ d'entrée. Celui-ci est intégré dans un code et est exécuté pour chaque jeu de données de la recherche LDAP.

Le serveur d'indexation ELO a une structure de données pour les utilisateurs et groupes : l'objet UserInfo. Celui-ci est décrit dans la documentation développeurs du serveur d'indexation ELO. L'accès dans le script de mappage peut se faire par le biais du nom de variable elo.

Mappage standard

- elo.type
- Selon LDAP `ObjectClass=person`
- Si la classe existe déjà, un utilisateur est créé, sinon, c'est un groupe qui est créé.
-

elo.name
- En fonction des attributs LDAP `displayName`, `cn`, `sAMAccounName` et `distinguishedName`
- Le premier attribut LDAP fait office de nom.
- `elo.userProps[UserInfoC.PROP_NAME_OS]`
- La valeur de l'attribut LDAP `sAMAccountName` est prise en charge.
- `elo.userProps[UserInfoC.PROP_NAME_EMAIL]`
- La valeur de l'attribut LDAP `mail` est copiée.
- `elo.superiorId`
- L'attribut LDAP `manager` est évalué.
- Lorsque l'attribut `manager` fait référence à un utilisateur ELO existant, son ID est entré en tant que supérieur.
- `elo.id`
- Si le nom se réfère à un utilisateur ELO valide, cet ID est entré comme ID ici. Sinon, -1 est utilisé pour un nouvel utilisateur.

Cadre du code JavaScript

Dans le niveau de rapport debug, le script créé est disponible dans le fichier journal.

```
// rhino compatible modus on java 8 (nashorn)
load('nashorn:mozilla_compat.js')
// editable basic javascript mapping function Version 1.0
importPackage(Packages.de.elo.ix.client)
importClass(Packages.de.elo.ldap.LdapImportException)
function extractDN(v){
try{
var vv=v.substring(3,v.indexOf('=', 3))
return vv.substring(0,vv.lastIndexOf(','))
}
catch(e){}
}
function map(ixc, elo, ldap, userNames){
%% Ici, le texte de l'interface est disponible pour le champ Script de mappage. %%
}
```

Lorsque la console d'administration ELO est démarrée sous Java 8, alors le mode de compatibilité Rhino est intégré.

```
public interface LdapImportMapping {
  public void map( de.elo.ix.client.IXConnection ixc, de.elo.ix.client.UserInfo userInfo, jav
}
```

L'accès au cadre JavaScript se fait par le biais de Java Interface `LdapImportMapping`. Dans mind map, le nom ELO est utilisé comme clé pour l'objet `UserName` (caractères minuscules).

Exemples

- Un jeu de données peut être exclu, en plaçant elo.id=0.

```
if (elo.name.startsWith("_")) {
  elo.id = 0
}
```

- Etant donné qu'il est possible d'utiliser JavaScript Code, il est également possible de faire afficher des versions pouvant être testées par le biais du mécanisme du message d'erreur.

```
throw ldap.get("mail").getClass()
```

ou aussi

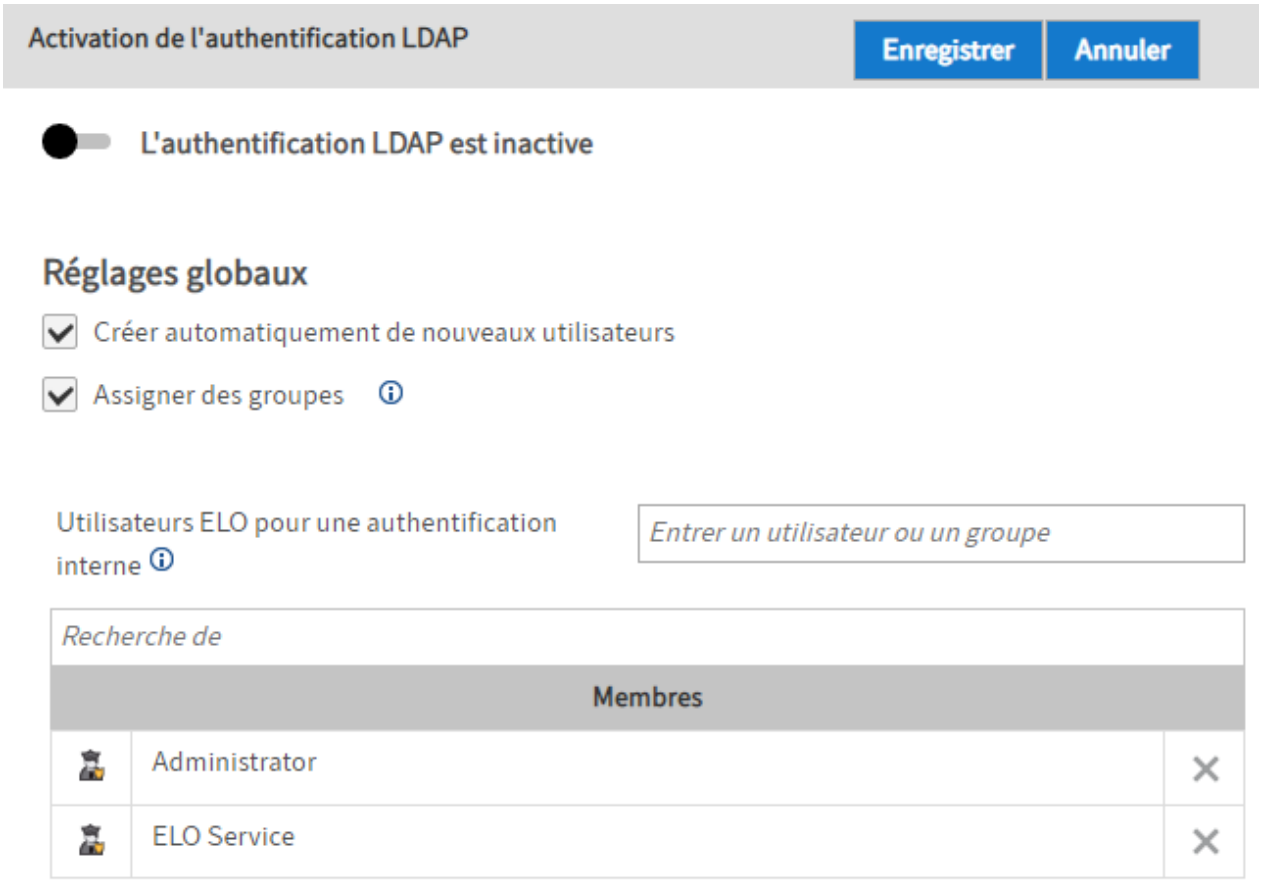
```
throw userNames["administrator"].id
```

- Notre exemple montre comment exclure des élément en vérifiant l'attribut `mail`, et comment le nom d'affichage est utilisé pour les utilisateurs restants.

```
var emailRegex = /^[\w._-]+[+]?[\w._-]+@[\w.-]+\.[a-zA-Z]{2,6}$/

var lMail = ldap.get("mail")
if (lMail) {
  lMail = lMail.get()
  if (emailRegex.test(lMail)) {
    elo.name += " (" + lMail.split("@").pop() + ")"
    // e-mail valide -> ajuster le nom d'affichage.
  }
} else {
  elo.id = 0
  // e-mail invalide -> uniquement
}
```

Activation de l'authentification LDAP



Authentification LDAP est inactive/Authentification LDAP est active : ce bouton permet d'activer ou de désactiver l'authentification LDAP.

Créer automatiquement les nouveaux utilisateurs : si l'option *Créer automatiquement les nouveaux utilisateurs* est activée, un utilisateur est créé automatiquement dans ELO, s'il n'existe pas encore.

> **Information**
>
> La première authentification (cela signifie que l'utilisateur n'existe pas encore dans ELO) doit se faire via une des valeurs suivantes :
>
> - `sAMAccountName`, `userPrincipalName` ou `mail` pour Active Directory
> - `UID` ou `mail` pour OpenLDAP

Assigner les groupes : si l'option *Assigner les groupes* est activée, les utilisateurs sont automatiquement assignés aux groupes LDAP correspondants. Pour ceci, les groupes doivent être créés dans ELO et les noms doivent correspondrent aux noms de groupe dans LDAP.

Remarque

Les groupes LDAP sont seulement extraits et appliqués lors de l'authentification des utilisateurs.

Utilisateur ELO pour l'authentification interne : ici, vous pouvez déterminer quels utilisateurs/groupes ne doivent pas pouvoir s'authentifier par LDAP. Vous pouvez authentifier ces utilisateurs/groupes directement à ELO.